Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP2006/313347

International filing date: 28 June 2006 (28.06.2006)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2005-189053
Filing date: 28 June 2005 (28.06.2005)

Date of receipt at the International Bureau: 03 August 2006 (03.08.2006)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００５年　６月２８日
出願番号 Application Number:	特願２００５－１８９０５３
パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号 The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is	ＪＰ２００５－１８９０５３
出願人 Applicant(s):	株式会社東芝 東芝ソリューション株式会社

２００６年　７月１９日

特許庁長官
Commissioner,
Japan Patent Office

中嶋　誠

【書類名】　特許願
【整理番号】　13B0560411
【提出日】　平成17年 6月28日
【あて先】　特許庁長官殿
【国際特許分類】　G11B 20/10
G06F 12/14
【発明者】
【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝　研究開発センター内
【氏名】　磯崎　宏
【発明者】
【住所又は居所】　東京都府中市片町３－２２
【氏名】　松川　伸一
【発明者】
【住所又は居所】　神奈川県横浜市磯子区新杉田町８番地　株式会社東芝　横浜事業所内
【氏名】　石原　淳
【発明者】
【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝　研究開発センター内
【氏名】　加藤　拓
【特許出願人】
【識別番号】　000003078
【氏名又は名称】　株式会社東芝
【特許出願人】
【識別番号】　301063496
【氏名又は名称】　東芝ソリューション株式会社
【代理人】
【識別番号】　100089118
【弁理士】
【氏名又は名称】　酒井　宏明
【手数料の表示】
【予納台帳番号】　036711
【納付金額】　16,000円
【提出物件の目録】
【物件名】　特許請求の範囲　1
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1

【書類名】特許請求の範囲
【請求項１】
番組の映像または音声のコンテンツである複数のタイトルコンテンツをタイトルコンテンツごとに暗号化する１つ以上のタイトルキーが登録されたタイトルキーファイルと、前記タイトルキーによって暗号化されたタイトルコンテンツとが記録された記録媒体の記録および再生を行うコンテンツ記録再生装置であって、
前記タイトルキーファイルを一つ以上生成し、一つ以上の前記タイトルキーを、生成された前記タイトルキーファイルに格納する初期化手段と、
複数のタイトルキーファイルのそれぞれに対応した第１の乱数を生成する第１の乱数生成手段と、
複数のタイトルキーファイルのそれぞれに対応した第２の乱数を生成する第２の乱数生成手段と、
前記初期化手段によって生成された前記タイトルキーファイルと前記第１の乱数と組にしてそれぞれ前記記録媒体に記録する記録手段と、を備え、
前記初期化手段は、前記複数のタイトルキーファイルのそれぞれを、前記第１の乱数生成手段によって生成され、前記タイトルキーファイルに対応した前記第１の乱数と関連づけられた他のタイトルキーファイルに登録された前記第２の乱数とによって前記タイトルキーを暗号化した暗号化タイトルキーと、前記タイトルキーファイルに対応した前記第１の乱数と前記他のタイトルキーファイルに登録された前記第２の乱数とを登録することによって生成することを特徴とするコンテンツ記録再生装置。
【請求項２】
前記記録媒体から前記複数のタイトルキーファイルを読み出す読み出し手段と、
前記記録媒体に記録された前記タイトルキーのリストに、新たなタイトルキーが追加された場合または前記タイトルキーのリストからタイトルキーが削除された場合に、前記読み出し手段によって読み出した前記複数のタイトルキーファイルの中で任意の前記タイトルキーファイルに登録された前記第１の乱数と前記タイトルキーファイルに関連付けられた他の前記タイトルキーファイルに登録された前記第２の乱数によって前記タイトルキーファイルに登録された前記暗号化タイトルキーを復号化し、前記第２の乱数を前記第２の乱数生成手段によって前記複数のタイトルキーファイルごとに新たに生成し、復号化された前記タイトルキーを、前記第１の乱数生成手段によって新たに生成された前記第１の乱数と他の前記タイトルキーファイルに対応して新たに生成された前記第２の乱数とによって前記タイトルキーファイルを暗号化する再暗号化手段と、
前記暗号化タイトルキーと前記第１の乱数と前記第２の乱数とを登録した前記タイトルキーファイルを複数生成することにより、前記複数のタイトルキーファイルを更新する更新手段と、をさらに備え、
前記記録手段は、前記更新手段によって更新された前記複数のタイトルキーファイルを前記記録媒体に記録することを特徴とする請求項１に記載のコンテンツ記録再生装置。
【請求項３】
前記記録媒体に記録された前記複数のタイトルキーファイルの中で、一つの前記タイトルキーファイルが存在しない場合あるいは破壊されている場合に、前記記録媒体に存在している前記タイトルキーファイルに登録された前記第１の乱数と前記タイトルキーファイルに関連付けられた他の前記タイトルキーファイルに登録された前記第２の乱数によって前記タイトルキーファイルに登録された前記暗号化タイトルキーを復号化し、前記第２の乱数を前記複数のタイトルキーファイルごとに新たに生成し、復号化された前記タイトルキーを、前記第１の乱数生成手段によって新たに生成された前記第１の乱数と他の前記タイトルキーファイルに対応して新たに生成された前記第２の乱数とによって暗号化する第２の再暗号化手段と、
前記暗号化タイトルキーと前記第１の乱数と前記第２の乱数とを登録した前記タイトルキーファイルを複数生成することによって、前記複数のタイトルキーファイルを回復する回復手段をさらに備え、

前記記録手段は、前記回復手段によって回復された前記複数のタイトルキーファイルを前記記録媒体に記録することを特徴とする請求項２に記載のコンテンツ記録再生装置。
【請求項４】
前記記録媒体は、任意の値を書き込むことが不可能なプロテクト領域と、任意のアプリケーションにより任意の値が記録可能なユーザ領域とを備え、
前記記録手段は、前記タイトルキーファイルの前記第１の乱数をプロテクト領域に記録し、前記第２の乱数を前記ユーザ領域に記録し、前記タイトルキーファイル以外のファイルを記録する場合には、前記プロテクト領域に正当な記録でない旨を示す不当情報を前記第１の乱数として記録する記録手段であって、
前記回復手段は、前記暗号化タイトルキーを復号化する際に、前記第１の乱数に前記不当情報が記録されているか否かを判断し、前記不当情報が記録されている場合には、前記複数のタイトルキーファイルの回復を行わないことを特徴とする請求項３に記載のコンテンツ記録再生装置。
【請求項５】
番組の映像または音声のコンテンツである複数のタイトルコンテンツをタイトルコンテンツごとに暗号化する１つ以上のタイトルキーが登録されたタイトルキーリストと、前記タイトルキーによって暗号化されたタイトルコンテンツとが記録された記録媒体の記録および再生を行うコンテンツ記録再生方法であって、
前記タイトルキーファイルを一つ以上生成し、一つ以上の前記タイトルキーを、生成された前記タイトルキーファイルに格納し、前記記録媒体に記録する初期化ステップと、
複数のタイトルキーファイルのそれぞれに対応した第１の乱数を生成する第１の乱数生成ステップと、
複数のタイトルキーファイルのそれぞれに対応した第２の乱数を生成する第２の乱数生成ステップと、
前記初期化ステップによって生成された前記タイトルキーファイルと前記第１の乱数とを組にしてそれぞれを前記記録媒体に記録する記録ステップと、を含み、
前記初期化ステップは、前記複数のタイトルキーファイルのそれぞれを、前記第１の乱数生成ステップによって生成され、前記タイトルキーファイルに対応した前記第１の乱数と関連づけられた他のタイトルキーファイルに登録された前記第２の乱数とによって前記タイトルキーを暗号化した暗号化タイトルキーと、前記タイトルキーファイルに対応した前記第１の乱数と前記他のタイトルキーファイルに登録された前記第２の乱数とを登録することによって生成することを特徴とするコンテンツ記録再生方法。
【請求項６】
番組の映像または音声のコンテンツである複数のタイトルコンテンツをタイトルコンテンツごとに暗号化する１つ以上のタイトルキーが登録されたタイトルキーリストと、前記タイトルキーによって暗号化されたタイトルコンテンツとが記録された記録媒体の記録および再生を行うコンテンツ記録再生プログラムであって、
前記タイトルキーファイルを一つ以上生成し、一つ以上の前記タイトルキーを、生成された前記タイトルキーファイルに格納し、前記記録媒体に記録する初期化ステップと、
複数のタイトルキーファイルのそれぞれに対応した第１の乱数を生成する第１の乱数生成ステップと、
複数のタイトルキーファイルのそれぞれに対応した第２の乱数を生成する第２の乱数生成ステップと、
前記初期化ステップによって生成された前記複数のタイトルキーファイルと前記第１の乱数とを組にしてそれぞれを前記記録媒体に記録する記録ステップと、をコンピュータに実行させ、
前記初期化ステップは、前記複数のタイトルキーファイルのそれぞれを、前記第１の乱数生成ステップによって生成され、前記タイトルキーファイルに対応した前記第１の乱数と関連づけられた他の前記タイトルキーファイルに登録された前記第２の乱数とによって前記タイトルキーファイルを暗号化した暗号化タイトルキーと、前記タイトルキーファイ

ルに対応した前記第１の乱数と前記他のタイトルキーファイルに登録された前記第２の乱数とを登録することによって生成することを特徴とするコンテンツ記録再生プログラム。

【書類名】明細書
【発明の名称】コンテンツ記録再生装置、コンテンツ記録再生方法およびコンテンツ記録再生プログラム
【技術分野】
【０００１】
本発明は、番組の映像または音声のコンテンツである複数のタイトルコンテンツをタイトルコンテンツごとに暗号化する複数のタイトルキーが登録されたタイトルキーファイルと、前記タイトルキーによって暗号化されたタイトルコンテンツとが記録された記録媒体の記録および再生を行うコンテンツ記録再生装置、コンテンツ記録再生方法およびコンテンツ記録再生プログラムに関し、特にタイトルキーファイルのバックアップ技術に関するものである。
【背景技術】
【０００２】
従来から、ＤＶＤ（Digital Versatile Disk）等の記録媒体に記録されたコンテンツの不正コピーを防止するため、番組の映像または音声のコンテンツである複数のタイトルコンテンツのそれぞれに対して、タイトルコンテンツごとに異なるタイトルキーで暗号化処理を施して、暗号化されたタイトルコンテンツをＤＶＤメディアに記録する技術が知られている（例えば、非特許文献１参照）。
【０００３】
この技術では、複数のタイトルキーのそれぞれを、コンテンツを正当に記録再生するＤＶＤレコーダ等の記録再生装置ごとに付与されたデバイスキーとランダムに発生させた乱数とにより暗号化して乱数とともにタイトルキーファイルに登録してＤＶＤメディアに記録している。そして、タイトルコンテンツを再生する場合には、このタイトルキーファイルに登録されている暗号化タイトルキーを乱数と再生しようとする記録再生装置のデバイスキーで復号化して復号化されたタイトルキーでタイトルコンテンツを復号化してタイトルコンテンツを再生している。
【０００４】
また、書き換え型のＤＶＤメディアにおいてタイトルコンテンツの一部を削除した場合には、タイトルキーファイルも更新する。具体的には、一度、タイトルキーファイルを復号化し、新たに乱数を生成し、デバイスキーでＤＶＤメディアから削除したタイトルコンテンツに対応するタイトルキーを削除したタイトルキーファイルを、新たな乱数とデバイスキーにより再度暗号化してＤＶＤメディアに記録している。これによって、削除したタイトルコンテンツに対応するタイトルキーを予め複製しておき、このタイトルキーを用いて削除したタイトルコンテンツを不正に再生する攻撃を防止することができる。
【０００５】
【非特許文献１】Advanced Access Content System (AACS) Recordable Video Book Revision 0.90
【発明の開示】
【発明が解決しようとする課題】
【０００６】
このようなタイトルキーを用いたコンテンツ保護は、ＤＶＤメディアのコンテンツの不正利用を防止するために有効な技術であるが、ＤＶＤメディアの汚れや傷等により一部の領域が読み出し不可能となり、タイトルキーファイルの読み出しができなくなった場合や、ユーザが誤ってタイトルキーファイルを消去してしまった場合には、タイトルコンテンツの復号化ができなくなり再生不可能となってしまう。このため、タイトルキーファイルの複製をバックアップファイルとしてＤＶＤメディアに記録しておき、タイトルキーファイルが壊れた等で読み出すことができない場合には、バックアップファイルをタイトルキーファイルとして使用することが考えられる。
【０００７】
しかしながら、タイトルキーファイルの単純なバックアップファイルをＤＶＤメディア

に記録しておくだけでは、コンテンツの不正な復元を許容してしまうことになる。すなわち、例えば、攻撃者が予めタイトルキーファイルのバックアップファイルを他のメディアにコピーしておいたとする。このとき、正規の手順でタイトルコンテンツの一部を他のメディアに移動した場合には、移動したタイトルコンテンツに対するタイトルキーを削除したタイトルキーファイルが更新される。このとき、攻撃者は、タイトルキーファイルをＤＶＤメディアから削除し、当該ＤＶＤメディアに他のメディアにコピーしておいたバックアップファイルを復元する。すると、記録再生装置は、本来のタイトルキーファイルがＤＶＤメディアに存在しないため、タイトルキーファイルをバックアップから復元するが、このバックアップファイルは更新前のタイトルキーファイルであるため、ＤＶＤメディアから削除したはずのタイトルコンテンツに対するタイトルキーが不正に復元されてしまうことになる。

【０００８】

本発明は、上記に鑑みてなされたものであって、タイトルキーファイルの復元を確実に行えるとともに、悪意のある第三者によるコンテンツの不正な復元を防止することができるコンテンツ記録再生装置、コンテンツ記録再生方法およびコンテンツ記録再生プログラムを提供することを目的とする。

【課題を解決するための手段】

【０００９】

上述した課題を解決し、目的を達成するために、本発明は、番組の映像または音声のコンテンツである複数のタイトルコンテンツをタイトルコンテンツごとに暗号化する１つ以上のタイトルキーが登録されたタイトルキーファイルと、前記タイトルキーによって暗号化されたタイトルコンテンツとが記録された記録媒体の記録および再生を行うコンテンツ記録再生装置であって、前記タイトルキーファイルを一つ以上生成し、一つ以上の前記タイトルキーを、生成された前記タイトルキーファイルに格納する初期化手段と、複数のタイトルキーファイルのそれぞれに対応した第１の乱数を生成する第１の乱数生成手段と、複数のタイトルキーファイルのそれぞれに対応した第２の乱数を生成する第２の乱数生成手段と、前記初期化手段によって生成された前記タイトルキーファイルと前記第１の乱数と組にしてそれぞれ前記記録媒体に記録する記録手段と、を備え、前記初期化手段は、前記複数のタイトルキーファイルのそれぞれを、前記第１の乱数生成手段によって生成され、前記タイトルキーファイルに対応した前記第１の乱数と関連づけられた他のタイトルキーファイルに登録された前記第２の乱数とによって前記タイトルキーを暗号化した暗号化タイトルキーと、前記タイトルキーファイルに対応した前記第１の乱数と前記他のタイトルキーファイルに登録された前記第２の乱数とを登録することによって生成することを特徴とする。また、本発明は、上記装置に対応したコンテンツ記録再生方法およびプログラムである。

【発明の効果】

【００１０】

本発明によれば、タイトルキーファイルを複数生成し、各タイトルキーファイルは、互いに他のタイトルキーファイルと関連付けされているため、タイトルキーファイルの復元を確実に行えるとともに、悪意のある第三者によるコンテンツの不正な復元を防止することができるという効果を奏する。

【発明を実施するための最良の形態】

【００１１】

以下に添付図面を参照して、コンテンツ記録再生装置、コンテンツ記録再生方法およびコンテンツ記録再生プログラムの最良な実施の形態を詳細に説明する。

【００１２】

（実施の形態１）

図１は、実施の形態１にかかるコンテンツ記録再生装置１００の構成を示すブロック図である。ここで、コンテンツ記録再生装置１００としては、例えば、ＤＶＤメディアへの記録および再生を行うＤＶＤレコーダ等があげられる。本実施の形態にかかるコンテンツ

記録再生装置１００は、図１に示すように、書き換え可能なＤＶＤメディア１４０にデータの機器録およびＤＶＤメディア１４０からのデータの読み出し等を行うドライブ部１１０と、タイトルコンテンツの暗号化と復号化およびタイトルキーファイル（ＴＫＦ：Title Key File）のバックアップ処理を行うホスト部１２０がバス１３０で接続された構成となっている。

【００１３】

ＤＶＤメディア１４０には、図１に示すように、後述するタイトルキーファイル（ＴＫＦ＃１）、タイトルキーファイルのバックアップファイルであるＴＫＦ＃２，ＴＫＦ＃３，乱数１～３が記録されている。

【００１４】

ここで、本実施の形態のコンテンツ記録再生装置１００で対象としているＤＶＤメディア１４０の形式は、ＨＤ　ＤＶＤ（High Density Digital Versatile Disk）　Ｖｉｄｅｏ　Ｒｅｃｏｒｄｉｎｇ規格に準拠したＤＶＤメディアであるが、必ずしもかかるフォーマットのＤＶＤメディアに限定されるものではない。

【００１５】

ドライブ部１１０は、ランダムに乱数を生成する乱数生成部１１１と、ＤＶＤメディア１４０からデータを直接読み出す読み出し部１１２と、ＤＶＤメディア１４０に対して、データを直接記録する記録部１１３とを主に備えている。

【００１６】

ホスト部１２０は、図１に示すように、コンテンツ暗号化処理部１２１と、コンテンツ復号化処理部１２２と、ＴＫＦ暗号化処理部１２３と、デバイス秘密鍵記憶部１２４と、バックアップ処理部１４０と、乱数生成部１２５を主に備えた構成となっている。

【００１７】

コンテンツ暗号化処理部１２１は、タイトルキーコンテンツをタイトルキーによって暗号化する処理部であり、コンテンツ復号化処理部１２２は、暗号化されたタイトルコンテンツをタイトルキーによって復号化する処理部である。

【００１８】

ここで、タイトルコンテンツは、番組としての映像や音声のコンテンツの単位であり、例えば、映画一本のコンテンツが一つのタイトルコンテンツとなる。タイトルキーは、このタイトルコンテンツを暗号化する鍵であり、タイトルコンテンツごとに異なる鍵となっている。なお、複数のタイトルが同一のタイトルキーで暗号化されていてもよい。

【００１９】

ＴＫＦ暗号化処理部１２３は、タイトルキーファイル（ＴＫＦ）を暗号化する処理部である。ここで、タイトルキーファイル（ＴＫＦ）は、１つ以上のタイトルキーを乱数とコンテンツ記録再生装置１００が有するデバイス秘密鍵とによって暗号化した１つ以上のタイトルキーの集合であり、かかるタイトルキーの集合と暗号化する際に使用した乱数が登録されたファイルである。タイトルキーファイルは、後述する乱数と、自身のタイトルキーファイルまたはバックアップファイル以外のファイルの暗号化されたタイトルキーを生成するためのＴＫＦ乱数と、１つ以上の暗号化されたタイトルキーとが登録されており、ＤＶＤメディア１４０に記録される。タイトルキーファイルの詳細は図４－１および図４－２にて後述する。

【００２０】

図１に戻り、デバイス秘密鍵記憶部１２４は、デバイス秘密鍵を記憶するメモリ等の記憶媒体である。ここで、デバイス秘密鍵とは、正規のコンテンツ記録再生装置１００に対して予め付与された秘密鍵であり、タイトルキーファイルのタイトルキーを暗号化および復号化するための鍵となっている。

【００２１】

ＴＫＦバックアップ処理部１４０は、ＤＶＤメディア１４０に記録されているタイトルキーファイル（ＴＫＦ）のバックアップ処理を行う処理部であり、ＴＫＦ初期化部１４１と、ＴＫＦ更新部１４２と、ＴＫＦ回復部１４３とを主に備えている。

【００２２】
ＴＫＦ初期化部１４１は、ＤＶＤメディア１４０に記録されたタイトルキーファイル（ＴＫＦ＃１）とバックアップファイルとしてのタイトルキーファイルＴＫＦ＃２、ＴＫＦ＃３を生成する処理部である。
【００２３】
ＴＫＦ更新部１４２は、ＤＶＤメディア１４０のタイトルコンテンツの一部が削除または追加となり、タイトルキーのリストに変更が起こった場合に、タイトルキーファイルが更新されるが、これに伴って、タイトルキーファイルＴＫＦ＃１とバックアップファイルとしてのタイトルキーファイルＴＫＦ＃２、ＴＫＦ＃３を再生成して更新する処理部である。
【００２４】
ＴＫＦ回復部１４３は、ＤＶＤメディア１４０のタイトルキーファイルＴＫＦ＃１またはバックアップファイルとしてのタイトルキーファイルＴＫＦ＃２、ＴＫＦ＃３のうち、どれか一つが破壊されていた場合、あるいは存在しなかった場合に、タイトルキーファイルＴＫＦ＃１、バックアップファイルとしてのタイトルキーファイルＴＫＦ＃２、ＴＫＦ＃３の中の一つからタイトルキーを再生してタイトルキーファイルおよびバックアップファイルとしてのタイトルキーファイルを回復する処理部である。乱数生成部１２５は、後述するＴＫＦ乱数を生成する処理部である。
【００２５】
次に、ＤＶＤメディア１４０のデータを構成するセクタの構造について説明する。データは、セクタと呼ばれる固定長のデータに分割されて、ＤＶＤメディア１４０に記録されている。そして、ＤＶＤメディア１４０上のあらゆるデータは、セクタ単位に読み出しおよび書き込みが行われる。図２は、セクタの構造を示す説明図である。１セクタは、図２に示すように、固定長Ｍバイトの管理用のセクタヘッダとＮバイトのデータとから構成される。そして、データは、任意のアプリケーションでリードライト可能なユーザ領域に記録され、セクタヘッダの一部は、外部から任意の値をライトできないプロテクト領域に記録される。外部から任意の値をライトできないようにする仕組みとして、図３に示すようなプロトコルを用いればよい。図３は、乱数をＤＶＤメディア１４０に書き込む処理の手順を示すシーケンス図である。
【００２６】
まず、ホスト部１２０からドライブ部１１０に乱数生成命令が送信される（ステップＳ３０１）。この乱数生成命令を受信したドライブ部１１０では乱数生成部１１１により乱数を生成し（ステップＳ３０２）、生成した乱数を一時的に蓄積しておく。次に、ホスト部１２０はドライブ部１１０に乱数書き込み命令を送信する（ステップＳ３０３）。ここで、乱数書き込み命令には乱数の値は含まれていない。数書き込み命令を受信したドライブ部１１０では、一次蓄積しておいた乱数を記録部１１３によってＤＶＤメディア１４０に書き込む（ステップＳ３０４）。このように、乱数書き込み命令に乱数の値を含まないようにすることで、ドライブ部１１０が生成した値以外の値をＤＶＤメディア１４０に書き込むことを防ぐことができる。
【００２７】
次に、本実施の形態のタイトルキーファイルのバックアップについて説明する。図４－１は、実施の形態１のタイトルキーファイルとバックアップファイルとしてのタイトルキーファイルの構造を示す説明図である。なお、以下においては説明の都合上、バックアップファイルとしてのタイトルキーファイルＴＫＦ＃２，ＴＫＦ＃３を単にバックアップファイルＴＫＦ＃２，ＴＫＦ＃３という。本実施の形態では、ＴＫＦ初期化部１４１によって、ＤＶＤメディア１４０に記録されたタイトルキーファイル（ＴＫＦ＃１）のバックアップファイルをＴＫＦ＃２，ＴＫＦ＃３として生成し、この３つのＴＫＦ＃１，ＴＫＦ＃２，ＴＫＦ＃３をドライブ部１１０の記録部１１３によってＤＶＤメディア１４０に格納している。
【００２８】

タイトルキーファイル（ＴＫＦ＃１）と各バックアップファイルＴＫＦ＃２，ＴＫＦ＃３は、乱数１～３（ＢＮ１，ＢＮ２，ＢＮ３）と、世代と、ＴＫＦ乱数１～３と、暗号化タイトルキー（ＥＴＫ１～３）とを登録した構成となっている。乱数１～３（ＢＮ１，ＢＮ２，ＢＮ３）は、ホスト部１２０の要求を受けてドライブ部１１０の乱数生成部１１１によってランダムに生成されてドライブ部１１０の記録部１１３によってＤＶＤメディア１４０上に記録される。世代は、タイトルキーファイル（ＴＫＦ＃１）およびバックアップファイルＴＫＦ＃２，ＴＫＦ＃３の変更回数を示すものである。

【００２９】

ＴＫＦ乱数１～３（ＴＫＦＮ１，ＴＫＦＮ２，ＴＫＦＮ３）は、自身のタイトルキーファイルまたはバックアップファイル以外のファイルの暗号化タイトルキー（ＥＴＫ１，ＥＴＫ２，ＥＴＫ３）を生成するための乱数である。ＴＫＦ乱数１～３はホスト部１２０の乱数生成部１２５によって生成される。

【００３０】

暗号化タイトルキー（ＥＴＫ１，ＥＴＫ２，ＥＴＫ３）は、タイトルキーファイルまたはバックアップファイルに登録されている乱数１～３（ＢＮ１，ＢＮ２，ＢＮ３）と、関連づけされている他のファイルに登録されているＴＫＦ乱数１～３（ＴＫＦＮ１，ＴＫＦＮ２，ＴＫＦＮ３）によって、タイトルキーファイルの全タイトルキーを暗号化したデータである。図４－２は、暗号化タイトルキー（ＥＴＫ１，ＥＴＫ２，ＥＴＫ３）の構造を示す説明図である。（ＥＴＫ１，ＥＴＫ２，ＥＴＫ３）は、図４－２に示すように、タイトルキー１～ｎのそれぞれを暗号化したものとなっている。暗号化タイトルキー（ＥＴＫ１，ＥＴＫ２，ＥＴＫ３）は、次の（１）～（３）式で示される。

【００３１】

ＥＴＫ１＝ｆ（ＴＫ，ＢＮ１，ＴＫＦＮ３）　・・・（１）

ＥＴＫ２＝ｆ（ＴＫ，ＢＮ２，ＴＫＦＮ１）　・・・（２）

ＥＴＫ３＝ｆ（ＴＫ，ＢＮ３，ＴＫＦＮ２）　・・・（３）

ここで、ＴＫは平文のタイトルキーを示し、ｆは、第１パラメタ（ＴＫ）に第２パラメタ（ＢＮ１～３）と第３パラメタ（ＴＫＦＮ１～３）を暗号鍵として暗号処理を施すことを示している。暗号処理ｆには、たとえばAES（Advanced Encryption Standard）などのよく知られた暗号アルゴリズムを用いればよい。

【００３２】

すなわち、ＴＫＦ＃１は、ＴＫＦ＃３と関連づけられており、タイトルキー（ＴＫ）を、乱数１（ＢＮ１）と、関連づけられたＴＫＦ＃３のＴＫＦ乱数３（ＴＫＦＮ３）とで暗号化したものとなっている。また、ＴＫＦ＃２は、ＴＫＦ＃１と関連づけられており、タイトルキー（ＴＫ）を、乱数２（ＢＮ２）と、関連づけられたＴＫＦ＃１のＴＫＦ乱数１（ＴＫＦＮ１）とで暗号化したものとなっている。さらに、ＴＫＦ＃３は、ＴＫＦ＃２と関連づけられており、タイトルキー（ＴＫ）を、乱数３（ＢＮ３）と、関連づけられたＴＫＦ＃２のＴＫＦ乱数２（ＴＫＦＮ２）とで暗号化したものとなっている。

【００３３】

このようにタイトルキーファイルＴＫＦ＃１と各バックアップファイルＴＫＦ＃２，ＴＫＦ＃３は、互いに他のファイルと関連付けられており、暗号化タイトルキー（ＥＴＫ１，ＥＴＫ２，ＥＴＫ３）は、自己のファイルに登録された乱数１～３（ＢＮ１，ＢＮ２，ＢＮ２）と、関連づけられている他のファイルに登録されているＴＫＦ乱数１～３（ＴＫＦＮ１，ＴＫＦＮ２，ＴＫＦＮ３）とでタイトルキー（ＴＫ）を暗号化したものとなっているので、悪意のある第三者が一つのバックアップファイルをコピーしてもタイトルキー（ＴＫ）を復元することができないようになっている。

【００３４】

なお、タイトルキーファイルと各バックアップファイルの他のファイルのＴＫＦ乱数との関連づけは、上記（１）～（３）式に限定されるものではなく、（１）～（３）式以外のパターンでタイトルキーファイルとバックアップファイルのＴＫＦ乱数と関連付けるように構成してもよい。

【００３５】
ここで、乱数１～３（ＢＮ１，ＢＮ２，ＢＮ３）は、タイトルキーファイルＴＫＦ＃１およびバックアップファイルＴＫＦ＃２，ＴＫＦ＃３が記録されたセクタの図３に示したプロテクト領域に記録される。一方、ＴＫＦ乱数１～３（ＴＫＦＮ１，ＴＫＦＮ２，ＴＫＦＮ３）はタイトルキーファイルＴＫＦ＃１およびバックアップファイルＴＫＦ＃２，ＴＫＦ＃３のユーザ領域に記録される。このため、乱数１～３（ＢＮ１，ＢＮ２，ＢＮ３）はユーザが任意の値を記録することができないが、ＴＫＦ乱数１～３（ＴＫＦＮ１，ＴＫＦＮ２，ＴＫＦＮ３）は、例えばエディタなどの鍵管理処理を行わないアプリケーションによって任意の値が書き込まれる場合もある。このため、本実施の形態では、タイトルキーファイルＴＫＦ＃１またはバックアップファイルＴＫＦ＃２，ＴＫＦ＃３を鍵管理処理を行わない一般のアプリケーションが編集（書き込み）を行う場合には、記録部１１３によって乱数１～３には不当情報として「０」を書き込むようになっている。例えば、ＴＫＦ＃１のＴＫＦＮ１に鍵管理処理を行わないアプリケーションが値を書き込む場合には、記録部１１３によってＢＮ１に０が設定されることになる。ＴＫＦ＃２、ＴＫＦ＃３についても同様である。
【００３６】
次に、以上のように構成された本実施の形態にかかるコンテンツ記録再生装置１００によるタイトルキーファイルのバックアップ処理について説明する。まず、タイトルキーファイル（ＴＫＦ）のバックアップの初期化処理について説明する。図５は、タイトルキーファイル（ＴＫＦ）のバックアップの初期化処理の手順を示すフローチャートである。
【００３７】
まず、ホスト部１２０はタイトルキー（ＴＫ）を生成する。そして、ＴＫＦ初期化部１４１では、乱数生成部１２５によってＴＫＦ乱数１～３（ＴＫＦＮ１，ＴＫＦＮ２，ＴＫＦＮ３）を乱数生成し（ステップＳ５０１）、世代も乱数生成する（ステップＳ５０２）。
【００３８】
次に、ＴＫＦ初期化部１４１は、ドライブ部１１０に保持されている乱数１（ＢＮ１）を取得する（ステップＳ５０３）。乱数１の生成・取得方法は、図３で示した方法で行う。そして、乱数１（ＢＮ１）と、関連付けされているＴＫＦ乱数３（ＴＫＦＮ３）から生成したタイトルキーを（１）式に従って暗号化し、暗号化タイトルキー（ＥＴＫ１）を生成する（ステップＳ５０４）。そして、ＴＫＦ初期化部１４１は、乱数１（ＢＮ１）とＴＫＦ乱数１（ＴＫＦＮ１）と世代と生成された暗号化タイトルキー（ＥＴＫ１）とからタイトルキーファイルＴＫＦ＃１を生成する（ステップＳ５０５）。生成したタイトルキーファイルＴＫＦ＃１は、ＴＫＦ初期化部１４１からドライブ部１１０に送られて記録部１１３によってＤＶＤメディア１４０に記録する（ステップＳ５０６）。
【００３９】
次に、ＴＫＦ初期化部１４１は、ドライブ部１１０に保持されている乱数２（ＢＮ２）を取得する（ステップＳ５０７）。乱数２の生成・取得方法は図３にて示した方法で行う。そして、乱数２（ＢＮ２）と、関連付けされているＴＫＦ乱数１（ＴＫＦＮ１）からタイトルキー（ＴＫ）を（２）式に従って暗号化し、暗号化タイトルキー（ＥＴＫ２）を生成する（ステップＳ５０８）。そして、ＴＫＦ初期化部１４１は、乱数２（ＢＮ２）とＴＫＦ乱数２（ＴＫＦＮ２）と世代と生成された暗号化タイトルキー（ＥＴＫ２）とからバックアップファイルＴＫＦ＃２を生成する（ステップＳ５０９）。生成したバックアップファイルＴＫＦ＃２は、ＴＫＦ初期化部１４１からドライブ部１１０に送られて記録部１１３によってＤＶＤメディア１４０に記録する（ステップＳ５１０）。
【００４０】
次に、ＴＫＦ初期化部１４１は、ドライブ部１１０に保持されている乱数３（ＢＮ３）を取得する（ステップＳ５１１）。乱数３の生成・取得方法は図３にて示した方法で行う。そして、乱数３（ＢＮ３）と、関連付けされているＴＫＦ乱数２（ＴＫＦＮ２）からタイトルキー（ＴＫ）を（３）式に従って暗号化し、暗号化タイトルキー（ＥＴＫ３）を生

成する（ステップＳ５１２）。そして、ＴＫＦ初期化部１４１は、乱数３（ＢＮ３）とＴＫＦ乱数３（ＴＫＦＮ３）と世代と生成された暗号化タイトルキー（ＥＴＫ３）とからバックアップファイルＴＫＦ＃３を生成する（ステップＳ５１３）。生成したバックアップファイルＴＫＦ＃３は、ＴＫＦ初期化部１４１からドライブ部１１０に送られて記録部１１３によってＤＶＤメディア１４０に記録する（ステップＳ５１４）。このようにしてＤＶＤメディア１４０上のタイトルキーは３つのファイルに格納されることになる。

【００４１】

次に、タイトルキーファイル（ＴＫＦ）のバックアップの更新処理について説明する。図６－１は、タイトルキーファイル（ＴＫＦ）のバックアップの更新処理の手順を示すフローチャートである。

【００４２】

バックアップファイルの更新処理は、ＤＶＤメディア１４０のタイトルコンテンツが削除されたり追加されることにより、タイトルキー（ＴＫ）のリストが更新された場合に実行される。このとき、読み出し部１１２によって、ＤＶＤメディア１４０からタイトルキー（ＴＫＦ＃１）と二つのバックアップファイルＴＫＦ＃２，ＴＫＦ＃３が読み出される。まず、タイトルキーファイル（ＴＫＦ＃１）と二つのバックアップファイルＴＫＦ＃２，ＴＫＦ＃３の世代フィールドの値が全て一致するかチェックする。一致していない場合は後述する回復処理を行う。一致している場合は、以下の処理を継続する。次に、ＴＫＦ更新部１４２は、ドライブ部１１０の読み出し部１１２からＤＶＤメディア１４０上に記録された乱数１（ＢＮ１）を取得する（ステップＳ６０１）。そして、タイトルキーファイルＴＫＦ＃１の暗号化タイトルキー（ＥＴＫ１）を、（１）式に従って、乱数１（ＢＮ１）と、関連づけされているＴＫＦ乱数＃３とによって復号化し（ステップＳ６０２）、タイトルキー（ＴＫ）を得る。そして、ＴＫＦ更新部１４２は、ＴＫＦ乱数１～３（ＴＫＦＮ１，ＴＫＦＮ２，ＴＫＦＮ３）を新たに乱数生成し（ステップＳ６０３）、世代を１増加して更新する（ステップＳ６０４）。

【００４３】

次に、ＴＫＦ更新部１４２はドライブ部１１０に乱数生成を要求して、乱数生成部１１１によって再生成された新たな乱数１（ＢＮ１）をドライブ部１１０から取得する（ステップＳ６０５）。そして、ＴＫＦ更新部１４２は、新たな乱数１（ＢＮ１）と、関連付けされた新たなＴＫＦ乱数３（ＴＫＦＮ３）から、タイトルキー（ＴＫ）を（１）式に従って暗号化し、暗号化タイトルキー（ＥＴＫ１）を生成する（ステップＳ６０６）。そして、ＴＫＦ更新部１４２は、新たな乱数１（ＢＮ１）と、新たなＴＫＦ乱数１（ＴＫＦＮ１）と更新された世代と生成された暗号化タイトルキー（ＥＴＫ１）とからタイトルキーファイルＴＫＦ＃１を生成し（ステップＳ６０７）、ＴＫＦ＃１を更新する。更新されたタイトルキーファイルＴＫＦ＃１は、ＴＫＦ更新部１４２からドライブ部１１０に送られて記録部１１３によってＤＶＤメディア１４０に記録する（ステップＳ６０８）。

【００４４】

上述したステップＳ６０１からＳ６０７までの処理を、ホスト部１２０とドライブ１１０との間のデータ送受信に着目して説明する。図６－２は、タイトルキーファイルＴＫＦ＃１を復号し、再生成した乱数１にて暗号化した後、ＴＫＦ＃１と再生成した乱数１をＤＶＤメディア１４０に書き込む処理の手順を示したシーケンス図である。まず、ホスト部１２０からドライブ部１１０に乱数読み出し命令が送信される（ステップＳ６２１）。この乱数読み出し命令を受信したドライブ部１１０では、読み出し部１１２によってＤＶＤメディア１４０から乱数１を読み込む（ステップＳ６２２）。そして、ドライブ部はＤＶＤメディア１４０から読み込んだ乱数１をホスト部１２０に送信する（ステップＳ６２３）。乱数１を受信したホスト部１２０ではＴＫＦ＃１の復号化処理が行われる（ステップＳ６２４）。

【００４５】

次いで、ホスト部１２０は、ドライブ部１１０に乱数生成命令を送信し（ステップＳ６２５）、乱数生成命令を受信したドライブ部１１０では乱数生成部１１１によって乱数１

を再生成し（ステップＳ６２６）、再生成した乱数１を一時的に蓄積しておく。ホスト部１２０からドライブ部１１０に乱数読み出し命令が送信されると（ステップＳ６２７）、ドライブ部１１０は一時的に蓄積された乱数１をホスト部１２０に送信する（ステップＳ６２８）。

【００４６】

再生成された乱数１を受信したホスト部１２０は、再生成された乱数1を用いてＴＫＦ＃１の暗号化処理を行う（ステップＳ６２９）。ＴＫＦ＃１の暗号化処理が終了したら、ホスト部１２０は、乱数書き込み命令（ＥＴＫ１）をドライブ部１１０に送信し（ステップＳ６３０）、ドライブ部１１０では、この乱数書き込み命令を受信すると、記録部１１３によって乱数１とＥＴＫ１をＤＶＤメディア１４０に書き込む（ステップＳ６３０）。

【００４７】

このようにＴＫＦ＃１と乱数１がＤＶＤメディア１４０に書き込まれると、図６－１に戻り、ＴＫＦ更新部１４２はドライブ部１１０に乱数生成を要求して、乱数生成部１１１によって再生成された新たな乱数２（ＢＮ２）をドライブ部１１０から取得する（ステップＳ６０９）。そして、ＴＫＦ更新部１４２は、新たな乱数２（ＢＮ２）と、関連付けされた新たなＴＫＦ乱数１（ＴＫＦＮ１）から、タイトルキー（ＴＫ）を（２）式に従って暗号化し、暗号化タイトルキー（ＥＴＫ２）を生成する（ステップＳ６１０）。そして、ＴＫＦ更新部１４２は、新たな乱数２（ＢＮ２）と、新たなＴＫＦ乱数２（ＴＫＦＮ２）と更新された世代と生成された暗号化タイトルキー（ＥＴＫ２）とからバックアップファイルＴＫＦ＃２を生成し（ステップＳ６１１）、ＴＫＦ＃２を更新する。更新されたバックアップファイルＴＫＦ＃２は、ＴＫＦ更新部１４２からドライブ部１１０に送られて記録部１１３によってＤＶＤメディア１４０に記録する（ステップＳ６１２）。

【００４８】

次に、ＴＫＦ更新部１４２はドライブ部１１０に乱数生成を要求して、乱数生成部１１１によって再生成された新たな乱数３（ＢＮ３）をドライブ部１１０から取得する（ステップＳ６１３）。そして、ＴＫＦ更新部１４２は、新たな乱数３（ＢＮ３）と、関連付けされた新たなＴＫＦ乱数２（ＴＫＦＮ２）からタイトルキー（ＴＫ）を（３）式に従って暗号化し、暗号化タイトルキー（ＥＴＫ３）を生成する（ステップＳ６１４）。そして、ＴＫＦ更新部１４２は、新たな乱数３（ＢＮ２）と新たなＴＫＦ乱数３（ＴＫＦＮ３）と更新された世代と生成された暗号化タイトルキー（ＥＴＫ３）とからバックアップファイルＴＫＦ＃３を生成し（ステップＳ６１５）、ＴＫＦ＃３を更新する。更新されたバックアップファイルＴＫＦ＃３は、ＴＫＦ更新部１４２からドライブ部１１０に送られて記録部１１３によってＤＶＤメディア１４０に記録する（ステップＳ６１６）。このようにして、タイトルキーファイルＴＫＦ＃１、バックアップファイルＴＫＦ＃２，ＴＫＦ＃３は更新され、ＴＫＦ＃１、ＴＫＦ＃２，ＴＫＦ＃３の順にＤＶＤメディア１４０に書き込まれることになる。このような順でタイトルキーファイルおよびバックアップファイルがＤＶＤメディア１４０に書き込まれることにより、世代の一致か不一致かによるバックアップファイルの回復の必要性の判断を行うことができる。

【００４９】

次に、タイトルキーファイル（ＴＫＦ＃１）およびバックアップファイル（ＴＫＦ＃２，ＴＫＦ＃３）のバックアップの回復処理について説明する。図７は、タイトルキーファイル（ＴＫＦ＃１）のバックアップの回復の全体処理の手順を示すフローチャートである。

【００５０】

バックアップファイルの回復処理は、ＤＶＤメディア１４０にタイトルキーファイルＴＫＦ＃１、バックアップファイルＴＫＦ＃２，ＴＫＦ＃３のいずれか１つが存在しない場合あるいは破壊されている場合、若しくは３つのファイルＴＫＦ＃１、ＴＫＦ＃２，ＴＫＦ＃３の世代が一致しない場合に実行される。具体的には、以下のような判断により行われる。

【００５１】

まず、読み出し部１１２によって、ＤＶＤメディア１４０からタイトルキーファイルＴＫＦ＃１およびバックアップファイルＴＫＦ＃２，ＴＫＦ＃３が読み出され、ＴＫＦ回復部１４３は、タイトルキーファイルＴＫＦ＃１が存在しないかあるいは破壊されているかを調べる（ステップＳ７０１）。そして、タイトルキーファイルＴＫＦ＃１が存在しないかあるいは破壊されている場合には（ステップＳ７０１：Ｙｅｓ）、バックアップファイルＴＫＦ＃３による回復処理を行う（ステップＳ７０８）。

【００５２】

一方、ステップＳ７０１において、タイトルキーファイルＴＫＦ＃１が存在し、かつ破壊されてない場合には（ステップＳ７０１：Ｎｏ）、バックアップファイルＴＫＦ＃２が存在しないかあるいは破壊されているかを調べる（ステップＳ７０２）。そして、バックアップファイルＴＫＦ＃２が存在しないかあるいは破壊されている場合には（ステップＳ７０２：Ｙｅｓ）、タイトルキーファイルＴＫＦ＃１による回復処理を行う（ステップＳ７０６）。

【００５３】

一方、ステップＳ７０２において、バックアップファイルＴＫＦ＃２が存在し、かつ破壊されてない場合には（ステップＳ７０２：Ｎｏ）、バックアップファイルＴＫＦ＃３が存在しないかあるいは破壊されているかを調べる（ステップＳ７０３）。そして、バックアップファイルＴＫＦ＃３が存在しないかあるいは破壊されている場合には（ステップＳ７０３：Ｙｅｓ）、バックアップファイルＴＫＦ＃２による回復処理を行う（ステップＳ７０７）。

【００５４】

一方、ステップＳ７０３において、バックアップファイルＴＫＦ＃３が存在し、かつ破壊されてない場合には（ステップＳ７０３：Ｎｏ）、ＴＫＦ＃１の世代がＴＫＦ＃２の世代（＝ＴＫＦ＃３の世代）より大きいか否かを調べる（ステップＳ７０４）。そして、ＴＫＦ＃１の世代がＴＫＦ＃２の世代（＝ＴＫＦ＃３の世代）より大きい場合には（ステップＳ７０４：Ｙｅｓ）、ＴＫＦ＃１の更新後、ＴＫＦ＃２の更新前にコンテンツ記録再生装置１００の電源断等により更新処理が中断したものと判断して、ＴＫＦ＃３による回復処理を行う（ステップＳ７０８）。

【００５５】

一方、ステップＳ７０４において、ＴＫＦ＃１の世代がＴＫＦ＃２の世代（＝ＴＫＦ＃３の世代）より大きくない場合には（ステップＳ７０４：Ｎｏ）、ＴＫＦ＃３の世代がＴＫＦ＃２の世代（＝ＴＫＦ＃１の世代）より小さいか否かを調べる（ステップＳ７０５）。そして、ＴＫＦ＃３の世代がＴＫＦ＃２の世代（＝ＴＫＦ＃１の世代）より小さい場合には（ステップＳ７０４：Ｙｅｓ）、ＴＫＦ＃２の更新後、ＴＫＦ＃３の更新前にコンテンツ記録再生装置１００の電源断等により更新処理が中断したものと判断して、ＴＫＦ＃２による回復処理を行う（ステップＳ７０７）。

【００５６】

一方、ステップＳ７０５において、ＴＫＦ＃３の世代がＴＫＦ＃２の世代（＝ＴＫＦ＃１の世代）より小さくない場合には（ステップＳ７０５：Ｎｏ）、いずれのバックアップファイルも存在し、かつ破壊されておらず、また更新中に更新処理が中断されていないため、バックアップファイルを回復する必要なしとして、回復処理を行わずに終了する。

【００５７】

次に、ステップＳ７０８におけるバックアップファイルＴＫＦ＃３による回復処理について説明する。図８は、バックアップファイルＴＫＦ＃３による回復処理の手順を示すフローチャートである。

【００５８】

ＴＫＦ回復部１４３は、ＴＫＦ＃１が存在しない場合か破壊されている場合、ＴＫＦ＃１の世代がＴＫＦ＃２およびＴＫＦ＃３の世代より大きい場合には、（３）式よりＴＫＦ＃３を用いて暗号化タイトルキー（ＥＴＫ３）を復号化して、タイトルキー（ＴＫ）を得て、このＴＫからＴＫＦ＃１、ＴＫＦ＃２、ＴＫＦ＃３の回復処理を行う。

【００５９】
このため、まず、ＴＫＦ回復部１４３は、ＴＫＦ＃２の乱数２（ＢＮ２）が格納されるプロテクト領域に不当情報としての０が設定されているか否かを調べる（ステップＳ８０１）。そして、ＴＫＦ＃２の乱数２（ＢＮ２）に０が設定されている場合には（ステップＳ８０１：Ｙｅｓ）、例えば、エディタなどのアプリケーションによりＴＫＦ＃２のユーザ領域にあるＴＫＦＮ２の値が変更され、不当な更新である場合があるので、エラー処理を行って（ステップＳ８１８）、回復処理を行わずに終了する。

【００６０】
一方、ステップＳ８０１において、ＴＫＦ＃２の乱数２（ＢＮ２）が格納されるプロテクト領域に０が設定されていない場合には（ステップＳ８０１：Ｎｏ）、ＴＫＦ＃２は正当なものであると判断して、以下の回復処理を続行する。

【００６１】
ＴＫＦ回復部１４３は、ドライブ部１１０からＤＶＤメディア１４０上に記録された乱数３（ＢＮ３）とＴＫＦ＃２，ＴＫＦ＃３を取得する（ステップＳ８０２）。そして、バックアップファイルＴＫＦ＃３の暗号化タイトルキー（ＥＴＫ３）を、乱数３（ＢＮ３）と、関連づけされているＴＫＦ乱数２（ＴＫＦＮ２）とによって（３）式によって復号化し（ステップＳ８０３）、タイトルキー（ＴＫ）を得る。そして、ＴＫＦ更新部１４２は、ＴＫＦ乱数１～３（ＴＫＦＮ１，ＴＫＦＮ２，ＴＫＦＮ３）を新たに乱数生成し（ステップＳ８０４）、世代を１増加して更新する（ステップＳ８０５）。

【００６２】
次に、ＴＫＦ回復部１４３はドライブ部１１０に乱数生成を要求して、乱数生成部１１１によって再生成された新たな乱数１（ＢＮ１）をドライブ部１１０から取得する（ステップＳ８０６）。そして、ＴＫＦ回復部１４３は、新たな乱数１（ＢＮ１）と、関連付けされた新たなＴＫＦ乱数３（ＴＫＦＮ３）からタイトルキー（ＴＫ）を（１）式に従って暗号化し、暗号化タイトルキー（ＥＴＫ１）を生成する（ステップＳ８０７）。そして、ＴＫＦ回復部１４３は、新たな乱数１（ＢＮ１）と、新たなＴＫＦ乱数１（ＴＫＦＮ１）と更新された世代と生成された暗号化タイトルキー（ＥＴＫ１）とからタイトルキーファイルＴＫＦ＃１を生成し（ステップＳ８０８）、ＴＫＦ＃１を回復する。回復されたタイトルキーファイルＴＫＦ＃１は、ＴＫＦ回復部１４３からドライブ部１１０に送られて記録部１１３によって乱数１（ＢＮ１）とともにＤＶＤメディア１４０に記録する（ステップＳ８０９）。

【００６３】
次に、ＴＫＦ回復部１４３はドライブ部１１０に乱数生成を要求して、乱数生成部１１１によって再生成された新たな乱数２（ＢＮ２）をドライブ部１１０から取得する（ステップＳ８１０）。そして、ＴＫＦ回復部１４３は、新たな乱数２（ＢＮ２）と、関連付けされた新たなＴＫＦ乱数１（ＴＫＦＮ１）からタイトルキー（ＴＫ）を（２）式に従って暗号化し、暗号化タイトルキー（ＥＴＫ２）を生成する（ステップＳ８１１）。そして、ＴＫＦ回復部１４３は、新たな乱数２（ＢＮ２）と、新たなＴＫＦ乱数２（ＴＫＦＮ２）と更新された世代と生成された暗号化タイトルキー（ＥＴＫ２）とからバックアップファイルＴＫＦ＃２を生成し（ステップＳ８１２）、ＴＫＦ＃２を回復する。回復されたバックアップファイルＴＫＦ＃２は、ＴＫＦ回復部１４３からドライブ部１１０に送られて記録部１１３によって乱数２（ＢＮ２）とともにＤＶＤメディア１４０に記録する（ステップＳ８１３）。

【００６４】
次に、ＴＫＦ回復部１４３はドライブ部１１０に乱数生成を要求して、乱数生成部１１１によって再生成された新たな乱数３（ＢＮ３）をドライブ部１１０から取得する（ステップＳ８１４）。そして、ＴＫＦ回復部１４３は、新たな乱数３（ＢＮ３）と、関連付けされた新たなＴＫＦ乱数２（ＴＫＦＮ２）からタイトルキー（ＴＫ）を（３）式に従って暗号化し、暗号化タイトルキー（ＥＴＫ３）を生成する（ステップＳ８１５）。そして、ＴＫＦ回復部１４３は、新たな乱数３（ＢＮ３）と、新たなＴＫＦ乱数３（ＴＫＦＮ３）

と更新された世代と生成された暗号化タイトルキー（ＥＴＫ３）とからバックアップファイルＴＫＦ＃３を生成し（ステップＳ８１６）、ＴＫＦ＃３を回復する。回復されたバックアップファイルＴＫＦ＃３は、ＴＫＦ回復部１４３からドライブ部１１０に送られて記録部１１３によって乱数３（ＢＮ３）とともにＤＶＤメディア１４０に記録する（ステップＳ８１７）。このようにして、ＴＫＦ＃３を用いて全てのバックアップファイルが回復されることになる。

【００６５】

次に、ステップＳ７０６におけるタイトルキーファイルＴＫＦ＃１による回復処理について説明する。図９は、タイトルキーファイルＴＫＦ＃１による回復処理の手順を示すフローチャートである。

【００６６】

ＴＫＦ回復部１４３は、ＴＫＦ＃２が存在しない場合か破壊されている場合には、（１）式よりＴＫＦ＃１を用いて暗号化タイトルキー（ＥＴＫ１）を復号化して、タイトルキー（ＴＫ）を得て、このＴＫからＴＫＦ＃１、ＴＫＦ＃２、ＴＫＦ＃３の回復処理を行う。

【００６７】

このため、まず、ＴＫＦ回復部１４３は、ＴＫＦ＃３の乱数３（ＢＮ３）に不当情報としての０が設定されているか否かを調べる（ステップＳ９０１）。そして、ＴＫＦ＃３の乱数３（ＢＮ３）に０が設定されている場合には（ステップＳ９０１：Ｙｅｓ）、例えば、エディタなどのアプリケーションによりＴＫＦ＃３のユーザ領域にあるＴＫＦＮ３の値が変更され、不当な更新である場合があるので、エラー処理を行って（ステップＳ９１８）、回復処理を行わずに終了する。

【００６８】

一方、ステップＳ９０１において、ＴＫＦ＃３の乱数３（ＢＮ３）に０が設定されていない場合には（ステップＳ９０１：Ｎｏ）、ＴＫＦ＃３は正当なものであると判断して、以下の回復処理を続行する。

【００６９】

ＴＫＦ回復部１４３は、ドライブ部１１０からＤＶＤメディア１４０上に記録された乱数１（ＢＮ１）とＴＫＦ＃１，ＴＫＦ＃３を取得する（ステップＳ９０２）。そして、タイトルキーファイルＴＫＦ＃１の暗号化タイトルキー（ＥＴＫ１）を、乱数１（ＢＮ１）と、関連づけされているＴＫＦ乱数３（ＴＫＦＮ３）とによって（１）式によって復号化し（ステップＳ９０３）、タイトルキー（ＴＫ）を得る。そして、ＴＫＦ更新部１４２は、ＴＫＦ乱数１～３（ＴＫＦＮ１，ＴＫＦＮ２，ＴＫＦＮ３）を新たに乱数生成し（ステップＳ９０４）、世代を１増加して更新する（ステップＳ９０５）。

【００７０】

これ以降のステップＳ９０６からＳ９１７までのＴＫＦ＃１、ＴＫＦ＃２、ＴＫＦ＃３の回復処理は、図８のステップＳ９０６からＳ９１７までの処理と同様に行われる。このようにして、ＴＫＦ＃１を用いて全てのバックアップファイルが回復されることになる。

【００７１】

次に、ステップＳ７０７におけるバックアップファイルＴＫＦ＃２による回復処理について説明する。図１０は、バックアップファイルＴＫＦ＃２による回復処理の手順を示すフローチャートである。

【００７２】

ＴＫＦ回復部１４３は、ＴＫＦ＃３が存在しない場合か破壊されている場合、ＴＫＦ＃３の世代がＴＫＦ＃２およびＴＫＦ＃１の世代より小さい場合には、（２）式よりＴＫＦ＃２を用いて暗号化タイトルキー（ＥＴＫ２）を復号化して、タイトルキーファイル（ＴＫＦ）を得て、このＴＫＦからＴＫＦ＃１、ＴＫＦ＃２、ＴＫＦ＃３の回復処理を行う。

【００７３】

このため、まず、ＴＫＦ回復部１４３は、ＴＫＦ＃１の乱数１（ＢＮ１）に不当情報としての０が設定されているか否かを調べる（ステップＳ１００１）。そして、ＴＫＦ＃１

の乱数１（ＢＮ１）に０が設定されている場合には（ステップＳ１００１：Ｙｅｓ）、例えば、エディタなどのアプリケーションによりＴＫＦ＃１のユーザ領域にあるＴＫＦＮ１の値が変更され、不当な更新である場合があるので、エラー処理を行って（ステップＳ１０１８）、回復処理を行わずに終了する。

【００７４】

一方、ステップＳ１００１において、ＴＫＦ＃１の乱数１（ＢＮ１）に０が設定されていない場合には（ステップＳ１００１：Ｎｏ）、ＴＫＦ＃１は正当なものであると判断して、以下の回復処理を続行する。

【００７５】

ＴＫＦ回復部１４３は、ドライブ部１１０からＤＶＤメディア１４０上に記録された乱数２（ＢＮ２）とＴＫＦ＃２，ＴＫＦ＃１を取得する（ステップＳ１００２）。そして、バックアップファイルＴＫＦ＃２の暗号化タイトルキー（ＥＴＫ２）を、乱数２（ＢＮ２）と、関連づけされているＴＫＦ乱数１（ＴＫＦＮ１）とによって（２）式によって復号化し（ステップＳ１００３）、タイトルキー（ＴＫ）を得る。そして、ＴＫＦ更新部１４２は、ＴＫＦ乱数１～３（ＴＫＦＮ１，ＴＫＦＮ２，ＴＫＦＮ３）を新たに乱数生成し（ステップＳ１００４）、世代を１増加して更新する（ステップＳ１００５）。

【００７６】

これ以降のステップＳ１００６からＳ１０１７までのＴＫＦ＃１、ＴＫＦ＃２、ＴＫＦ＃３の回復処理は、図８のステップＳ９０６からＳ９１７までの処理と同様に行われる。このようにして、ＴＫＦ＃２を用いて全てのバックアップファイルが回復されることになる。

【００７７】

このように実施の形態１では、タイトルキー（ＴＫ）の暗号化ファイルを３つ用意し、それぞれの暗号化タイトルキーを、自己の乱数と自己と関連付けられた他のファイルのＴＫＦ乱数によって（１）～（３）式のように暗号化している。このため、例えば、攻撃者が予め１つのバックアップファイルを他のメディアにコピーしておき、正規の手順でタイトルコンテンツの一部を他のメディアに移動して、タイトルキーファイルが更新され、攻撃者がタイトルキーファイルをＤＶＤメディアから削除し、当該ＤＶＤメディアに他のメディアにコピーしておいたバックアップファイルを復元したとしても、少なくとも２個のファイルがなければ、（１）～（３）式よりタイトルキーを復号化できず、また他の２つのファイルは更新処理によって更新されているので、結局タイトルキーを復元することができない。このため、ＤＶＤメディアから削除したタイトルコンテンツに対するタイトルキーを不正に復元されてしまうことを防止し、タイトルコンテンツの不正な利用を防止することができる。

【００７８】

また、例えば、攻撃者が予め１つのバックアップファイルをリネームして同一のDVDメディアに保存した場合でも、タイトルキーファイルを作成するアプリケーションではないアプリケーションが、タイトルキーファイルを編集した場合、プロテクト領域に記録される乱数１～３に不当情報である０が設定されてしまうので、バックアップファイルの不当な回復処理が実行されず、結局タイトルキーを復元することができない。このため、タイトルコンテンツの不正な利用を防止することができる。

【００７９】

（変形例）

実施の形態１では、タイトルキーファイルＴＫＦ＃１およびバックアップファイルＴＫＦ＃２，ＴＫＦ＃３の世代は、初期化時に乱数生成し、タイトルコンテンツが削除されたり追加されたりするなどによりタイトルキーのリストが変化するたびに、更新処理の一貫として世代を１ずつ更新するように構成されていた。しかし、世代を、初期化時に限らず更新処理に毎回乱数生成するように構成してもよい。図１１は、世代を更新処理時に毎回乱数生成した場合におけるタイトルキーファイル（ＴＫＦ）のバックアップの回復処理の全体処理の手順を示すフローチャートである。

【００８０】
かかるバックアップ回復の全体処理では、ステップＳ１１０４とＳ１１０５のみが図７で説明した全体処理と異なっている。すなわち、ステップＳ１１０４では、ＴＫＦ＃２とＴＫＦ＃３の世代の値は一致するが、ＴＫＦ＃２およびＴＫＦ＃３の世代の値がＴＫＦ＃１の世代の値と一致しないかとうかを判断している。また、ステップＳ１１０５では、ＴＫＦ＃１とＴＫＦ＃２の世代の値は一致するが、ＴＫＦ＃１およびＴＫＦ＃２の世代の値とＴＫＦ＃３の世代の値とは一致しないかとうかを判断している。これは、本変形例では、更新処理ごとに毎回、世代を乱数生成しているためである。
【００８１】
（実施の形態２）
実施の形態１では、タイトルキーファイルＴＫＦ＃１、バックアップファイルＴＫＦ＃２，ＴＫＦ＃３の構造が図４－１に示すように同一であったが、この実施の形態２では、バックアップファイルＴＫＦ＃３の構造がタイトルキーファイルＴＫＦ＃１およびバックアップファイルＴＫＦ＃２と異なっている。
【００８２】
実施の形態２にかかる記録再生装置の構成は、図１で説明した実施の形態１の記録再生装置と同様である。
【００８３】
図１２は、実施の形態２のタイトルキーファイルとバックアップファイルの構造を示す説明図である。本実施の形態では、バックアップファイルＴＫＦ＃３が暗号化タイトルキーとＴＫＦ乱数３を有さず、その代わりに、ＴＫＦ乱数１（ＴＫＦＮ１）とＴＫＦ乱数２（ＴＫＦＮ２）を備えている点、およびタイトルキーファイルＴＫＦ＃１の暗号化タイトルキー（ＥＴＫ１）とバックアップファイルＴＫＦ＃２の暗号化タイトルキー（ＥＴＫ２）の計算方式が実施の形態１と異なっている。
【００８４】
タイトルキーファイルＴＫＦ＃１とバックアップファイルＴＫＦ＃２は、実施の形態１のＴＫＦ＃１，ＴＫＦ＃２と同様に、乱数１，２（ＢＮ１，ＢＮ２）と、世代と、ＴＫＦ乱数１，２（ＴＫＦＮ１，ＴＫＦＮ２）と暗号化タイトルキー（ＥＴＫ１，ＥＴＫ２）から構成されている。ＴＫＦ＃１のＴＫＦ乱数１（ＴＫＦＮ１）は、ＴＫＦ＃１自身以外のバックアップファイルＴＫＦ＃２の暗号化タイトルキー（ＥＴＫ２）を生成するための乱数である。ＴＫＦ＃２のＴＫＦ乱数２（ＴＫＦＮ２）は、ＴＫＦ＃２自身以外のＴＫＦ＃１の暗号化タイトルキー（ＥＴＫ１）を生成するための乱数である。
【００８５】
バックアップファイルＴＫＦ＃３は、ＴＫＦ＃１およびＴＫＦ＃２の構造と異なり、乱数３（ＢＮ３）と、世代と、ＴＫＦ乱数１（ＴＫＦＮ１）と、ＴＫＦ乱数２（ＴＫＦＮ２）とを有している。このＴＫＦ＃３のＴＫＦ乱数のうち、ＴＫＦＮ１は，タイトルキーファイルＴＫＦ＃１のＴＫＦ乱数１（ＴＫＦＮ１）と同じ値が記録され、ＴＫＦＮ２は，バックアップファイルＴＫＦ＃２のＴＫＦ乱数２（ＴＫＦＮ２）と同じ値が記録される。
【００８６】
暗号化タイトルキー（ＥＴＫ１，ＥＴＫ２）は、タイトルキーファイルＴＫＦ＃１またはバックアップファイルＴＫＦ＃２，ＴＫＦ＃３に登録されている乱数（ＢＮ１，ＢＮ２）と、関連づけされている他のファイルに登録されているＴＫＦ乱数（ＴＫＦＮ１，ＴＫＦＮ２）によって、タイトルキーファイルの全タイトルキーを暗号化したデータである。暗号化タイトルキー（ＥＴＫ１，ＥＴＫ２）は、次の（４），（５）式で示される。
【００８７】
ＥＴＫ１＝ｆ（ＴＫ，ＢＮ１，ＴＫＦＮ２）　・・・（４）
ＥＴＫ２＝ｆ（ＴＫ，ＢＮ２，ＴＫＦＮ１）　・・・（５）
ここで、ＴＫはタイトルキーを示し、ｆは、第１パラメタ（ＴＫ）に第２パラメタ（ＢＮ１，２）と第３パラメタ（ＴＫＦＮ１，２）を暗号鍵として暗号処理を施すことを示している。暗号処理ｆには、たとえばＡＥＳ（Advanced Encryption Standard）などのよく

知られた暗号アルゴリズムを用いればよい。

【００８８】

次に、以上のように構成された本実施の形態にかかるコンテンツ記録再生装置１００によるタイトルキーファイルのバックアップ処理について説明する。

【００８９】

まず、タイトルキーファイル（ＴＫＦ）のバックアップの初期化処理について説明する。図１３は、タイトルキーファイル（ＴＫＦ）のバックアップの初期化処理の手順を示すフローチャートである。本実施の形態のバックアップ初期化処理では、バックアップファイルＴＫＦ＃３の構造が図１２に示すとおりＴＫＦ＃１、ＴＫＦ＃２と異なり、また暗号化タイトルキー（ＥＴＫ１，ＥＴＫ２）が（４）、（５）式で求められることから、タイトルキーファイルＴＫＦ＃１の暗号化タイトルキー（ＥＴＫ１）の生成処理と、タイトルキーファイルＴＫＦ＃１の生成処理と、バックアップファイルＴＫＦ＃３の生成処理が図５で説明した実施の形態１のバックアップ初期化処理と異なっている。

【００９０】

まず、ホスト部１２０はタイトルキー（ＴＫ）を生成する。そして、ＴＫＦ初期化部１４１は、乱数生成部１２５によってＴＫＦ乱数１，２（ＴＫＦＮ１，ＴＫＦＮ２）を乱数生成し（ステップＳ１３０１）、世代も乱数生成する（ステップＳ１３０２）。

【００９１】

次に、ＴＫＦ初期化部１４１は、ドライブ部１１０で保持されている乱数１（ＢＮ１）を取得する（ステップＳ５０３）。ここで乱数１の生成・取得方法は、図３で示した方法で行う。そして、乱数１（ＢＮ１）と、関連付けされているＴＫＦ乱数２（ＴＫＦＮ２）から、生成したタイトルキーを（４）式に従って暗号化し、暗号化タイトルキー（ＥＴＫ１）を生成する（ステップＳ１３０４）。そして、ＴＫＦ初期化部１４１は、乱数１（ＢＮ１）とＴＫＦ乱数１（ＴＫＦＮ１）と世代と生成された暗号化タイトルキー（ＥＴＫ１）とからタイトルキーファイルＴＫＦ＃１を生成する（ステップＳ１３０５）。生成したタイトルキーファイルＴＫＦ＃１は、ＴＫＦ初期化部１４１からドライブ部１１０に送られて記録部１１３によってＤＶＤメディア１４０に記録する（ステップＳ１３０６）。

【００９２】

次に、ＴＫＦ初期化部１４１は、ドライブ部１１０で保持されている乱数２（ＢＮ２）を取得する（ステップＳ５０７）。ここで、乱数２の生成・取得方法は図３にて示した方法で行う。そして、乱数２（ＢＮ２）と、関連付けされているＴＫＦ乱数１（ＴＫＦＮ１）からタイトルキー（ＴＫ）を（５）式に従って暗号化し、暗号化タイトルキー（ＥＴＫ２）を生成する（ステップＳ１３０８）。そして、ＴＫＦ初期化部１４１は、乱数２（ＢＮ２）とＴＫＦ乱数２（ＴＫＦＮ２）と世代と生成された暗号化タイトルキー（ＥＴＫ２）とからバックアップファイルＴＫＦ＃２を生成する（ステップＳ１３０９）。生成したバックアップファイルＴＫＦ＃２は、ＴＫＦ初期化部１４１からドライブ部１１０に送られて記録部１１３によってＤＶＤメディア１４０に記録する（ステップＳ１３１０）。

【００９３】

次に、ＴＫＦ初期化部１４１は、ドライブ部１１０で保持されている乱数３（ＢＮ３）を取得する（ステップＳ１３１１）。乱数３の生成・取得方法は図３にて示した方法で行う。そして、乱数３（ＢＮ３）とＴＫＦ乱数１（ＴＫＦＮ１）とＴＫＦ乱数２（ＴＫＦＮ２）と世代とから図１２に示す構造のバックアップファイルＴＫＦ＃３を生成する（ステップＳ１３１２）。生成したバックアップファイルＴＫＦ＃３は、ＴＫＦ初期化部１４１からドライブ部１１０に送られて記録部１１３によってＤＶＤメディア１４０に記録する（ステップＳ１３１３）。以上のような処理で、図１２に示すタイトルキーファイルＴＫＦ＃１、バックアップファイルＴＫＦ＃２，ＴＫＦ＃３が生成される。

【００９４】

次に、タイトルキーファイル（ＴＫＦ）のバックアップの更新処理について説明する。図１４は、実施の形態２におけるタイトルキーファイル（ＴＫＦ）のバックアップの更新処理の手順を示すフローチャートである。本実施の形態では、バックアップファイルＴＫ

Ｆ＃３の構造が図１２に示すとおりＴＫＦ＃１、ＴＫＦ＃２と異なり、また暗号化タイトルキー（ＥＴＫ１，ＥＴＫ２）が（４）、（５）式で求められることからタイトルキーファイル（ＴＫＦ＃１）の復号化処理、タイトルキーファイルＴＫＦ＃１の暗号化タイトルキー（ＥＴＫ１）の生成処理、タイトルキーファイルＴＫＦ＃１の生成処理、バックアップファイルＴＫＦ＃３の生成処理が図６－１で説明した実施の形態１の更新処理と異なっている。

【００９５】

本実施の形態でもバックアップファイルの更新処理は、ＤＶＤメディア１４０のタイトルコンテンツが削除されたり追加されることにより、タイトルキー（ＴＫ）のリストが更新された場合に実行される。このとき、読み出し部１１２によって、ＤＶＤメディア１４０からタイトルキー（ＴＫＦ＃１）と二つのバックアップファイルＴＫＦ＃２，ＴＫＦ＃３が読み出される。まず、ＴＫＦ更新部１４２は、ドライブ部１１０の読み出し部１１２からＤＶＤメディア１４０上に記録された乱数１（ＢＮ１）を取得する（ステップＳ１４０１）。そして、タイトルキーファイルＴＫＦ＃１の暗号化タイトルキー（ＥＴＫ１）を、（４）式に従って、乱数１（ＢＮ１）と関連づけされているＴＫＦ乱数＃２とによって復号化し（ステップＳ１４０２）、タイトルキー（ＴＫ）を得る。そして、ＴＫＦ更新部１４２は、ＴＫＦ乱数１（ＴＫＦＮ１）およびＴＫＦ乱数２（ＴＫＦＮ２）を新たに乱数生成し（ステップＳ１４０３）、世代を１増加して更新する（ステップＳ１４０４）。

【００９６】

次に、ＴＫＦ更新部１４２は、ドライブ部１１０に乱数生成を要求して、乱数生成部１１１によって再生成された新たな乱数１（ＢＮ１）をドライブ部１１０から取得する（ステップＳ１４０５）。そして、ＴＫＦ更新部１４２は、新たな乱数１（ＢＮ１）と、関連付けされた新たなＴＫＦ乱数２（ＴＫＦＮ２）から、タイトルキー（ＴＫ）を（４）式に従って暗号化し、暗号化タイトルキー（ＥＴＫ１）を生成する（ステップＳ１４０６）。そして、ＴＫＦ更新部１４２は、新たな乱数１（ＢＮ１）と、新たなＴＫＦ乱数１（ＴＫＦＮ１）と更新された世代と生成された暗号化タイトルキー（ＥＴＫ１）とからタイトルキーファイルＴＫＦ＃１を生成し（ステップＳ１４０７）、ＴＫＦ＃１を更新する。更新されたタイトルキーファイルＴＫＦ＃１は、ＴＫＦ更新部１４２からドライブ部１１０に送られて記録部１１３によってＤＶＤメディア１４０に記録する（ステップＳ１４０８）。

【００９７】

次に、ＴＫＦ更新部１４２はドライブ部１１０に乱数生成を要求して、乱数生成部１１１によって再生成された新たな乱数２（ＢＮ２）をドライブ部１１０から取得する（ステップＳ１４０９）。そして、ＴＫＦ更新部１４２は、新たな乱数２（ＢＮ２）と、関連付けされた新たなＴＫＦ乱数１（ＴＫＦＮ１）から、タイトルキー（ＴＫ）を（５）式に従って暗号化し、暗号化タイトルキー（ＥＴＫ２）を生成する（ステップＳ１４１０）。そして、ＴＫＦ更新部１４２は、新たな乱数２（ＢＮ２）と、新たなＴＫＦ乱数２（ＴＫＦＮ２）と更新された世代と生成された暗号化タイトルキー（ＥＴＫ２）とからバックアップファイルＴＫＦ＃２を生成し（ステップＳ１４１１）、ＴＫＦ＃２を更新する。更新されたバックアップファイルＴＫＦ＃２は、ＴＫＦ更新部１４２からドライブ部１１０に送られて記録部１１３によってＤＶＤメディア１４０に記録する（ステップＳ１４１２）。

【００９８】

次に、ＴＫＦ更新部１４２は、ドライブ部１１０に乱数生成を要求して、乱数生成部１１１によって再生成された新たな乱数３（ＢＮ３）をドライブ部１１０から取得する（ステップＳ１４１３）。そして、ＴＫＦ更新部１４２は、新たな乱数３（ＢＮ３）と、更新された世代と、新たなＴＫＦ乱数１（ＴＫＦＮ１）と、新たなＴＫＦ乱数２（ＴＫＦＮ２）とから、図１２に示す構造のバックアップファイルＴＫＦ＃３を生成し（ステップＳ１４１４）、ＴＫＦ＃３を更新する。更新されたバックアップファイルＴＫＦ＃３は、ＴＫＦ更新部１４２からドライブ部１１０に送られて記録部１１３によってＤＶＤメディア１４０に記録する（ステップＳ１４１５）。このようにして、タイトルキーファイルＴＫＦ

＃１、バックアップファイルＴＫＦ＃２，ＴＫＦ＃３は更新され、ＴＫＦ＃１、ＴＫＦ＃２，ＴＫＦ＃３の順にＤＶＤメディア１４０に書き込まれることになる。

【００９９】

次に、タイトルキーファイル（ＴＫＦ＃１）およびバックアップファイル（ＴＫＦ＃２，ＴＫＦ＃３）のバックアップの回復処理について説明する。図１５は、タイトルキーファイル（ＴＫＦ＃１）のバックアップの回復の全体処理の手順を示すフローチャートである。本実施の形態では、バックアップファイルＴＫＦ＃３の構造が図１２に示すとおりＴＫＦ＃１、ＴＫＦ＃２と異なり、また暗号化タイトルキー（ＥＴＫ１，ＥＴＫ２）が（４）、（５）式で求められることから、各回復処理において用いるファイルが実施の形態１の回復処理と異なっている。

【０１００】

すなわち、ステップＳ１５０１からＳ１５０５までの判断処理は、図７で説明したステップＳ７０１からＳ７０５までの処理と同様に行われる。本実施の形態では、ステップＳ１５０２でＴＫＦ＃２が存在しない場合あるいは破壊されている場合には、ＴＫＦ＃１、ＴＫＦ＃３を用いた回復処理が行われる（ステップＳ１５０６）。また、ステップＳ１５０３でＴＫＦ＃３が存在しない場合あるいは破壊されている場合、ステップＳ１５０５でＴＫＦ＃３の世代がＴＫＦ＃１およびＴＫＦ＃２の世代より小さい場合には、ＴＫＦ＃１、ＴＫＦ＃２を用いた回復処理が行われる（ステップＳ１５０７）。さらに、ステップＳ１５０１でＴＫＦ＃１が存在しない場合あるいは破壊されている場合、またはステップＳ１５０４でＴＫＦ＃１の世代がＴＫＦ＃２およびＴＫＦ＃３の世代より大きい場合、ＴＫＦ＃２、ＴＫＦ＃３を用いた回復処理が行われる（ステップＳ１５０８）。

【０１０１】

次に、ステップＳ１５０８におけるバックアップファイルＴＫＦ＃２の暗号化タイトルキー（ＥＴＫ２）を復号することによる回復処理について説明する。図１６は、バックアップファイルＴＫＦ＃２、＃３による回復処理の手順を示すフローチャートである。本実施の形態では、バックアップファイルＴＫＦ＃２を用いてバックアップファイルＴＫＦ＃３の乱数３が不当情報（「０」）として設定されているか否かを調べている点、バックアップファイルＴＫＦ＃２の暗号化タイトルキー（ＥＴＫ２）の復号処理、タイトルキーファイルＴＫＦ＃１の暗号化タイトルキー（ＥＴＫ１）の生成処理、タイトルキーファイルＴＫＦ＃１の生成処理、バックアップファイルＴＫＦ＃３の生成処理が、図８で説明した実施の形態１のＴＫＦ＃３による回復処理と異なっている。

【０１０２】

まず、ＴＫＦ回復部１４３は、ＴＫＦ＃３の乱数３（ＢＮ３）が格納されるプロテクト領域に不当情報としての０が設定されているか否かを調べる（ステップＳ１６０１）。そして、ＴＫＦ＃３の乱数３（ＢＮ３）に０が設定されている場合には（ステップＳ１６０１：Ｙｅｓ）、例えば、エディタなどのアプリケーションによりＴＫＦ＃３のユーザ領域にあるＴＫＦＮ１，ＴＫＦＮ２の値が変更され、不当な更新である場合があるので、エラー処理を行って（ステップＳ１６１７）、回復処理を行わずに終了する。

【０１０３】

一方、ステップＳ１６０１において、ＴＫＦ＃３の乱数３（ＢＮ３）が格納されるプロテクト領域に０が設定されていない場合には（ステップＳ１６０１：Ｎｏ）、ＴＫＦ＃３は正当なものであると判断して、以下の回復処理を続行する。

【０１０４】

ＴＫＦ回復部１４３は、ドライブ部１１０からＤＶＤメディア１４０上に記録された乱数２（ＢＮ２）とＴＫＦ＃２，ＴＫＦ＃３を取得する（ステップＳ１６０２）。そして、バックアップファイルＴＫＦ＃２の暗号化タイトルキー（ＥＴＫ２）を、乱数２（ＢＮ２）と、ＴＫＦ＃３に格納されているＴＫＦ乱数１（ＴＫＦＮ１）とによって（５）式によって復号化し（ステップＳ１６０３）、タイトルキー（ＴＫ）を得る。そして、ＴＫＦ更新部１４２は、ＴＫＦ乱数１、２（ＴＫＦＮ１，ＴＫＦＮ２）を新たに乱数生成し（ステップＳ１６０４）、世代を１増加して更新する（ステップＳ１６０５）。

【０１０５】
次に、ＴＫＦ回復部１４３はドライブ部１１０に乱数生成を要求して、乱数生成部１１１によって再生成された新たな乱数１（ＢＮ１）をドライブ部１１０から取得する（ステップＳ１６０６）。そして、ＴＫＦ回復部１４３は、新たな乱数１（ＢＮ１）と、関連付けされた新たなＴＫＦ乱数２（ＴＫＦＮ２）からタイトルキー（ＴＫ）を（４）式に従って暗号化し、暗号化タイトルキー（ＥＴＫ１）を生成する（ステップＳ１６０７）。そして、ＴＫＦ回復部１４３は、新たな乱数１（ＢＮ１）と、新たなＴＫＦ乱数１（ＴＫＦＮ１）と更新された世代と生成された暗号化タイトルキー（ＥＴＫ１）とからタイトルキーファイルＴＫＦ＃１を生成し（ステップＳ１６０８）、ＴＫＦ＃１を回復する。回復されたタイトルキーファイルＴＫＦ＃１は、ＴＫＦ回復部１４３からドライブ部１１０に送られて乱数１（ＢＮ１）とともに記録部１１３によってＤＶＤメディア１４０に記録する（ステップＳ１６０９）。
【０１０６】
次に、ＴＫＦ回復部１４３はドライブ部１１０に乱数生成を要求して、乱数生成部１１１によって再生成された新たな乱数２（ＢＮ２）をドライブ部１１０から取得する（ステップＳ１６１０）。そして、ＴＫＦ回復部１４３は、新たな乱数２（ＢＮ２）と、関連付けされた新たなＴＫＦ乱数１（ＴＫＦＮ１）からタイトルキー（ＴＫ）を（５）式に従って暗号化し、暗号化タイトルキー（ＥＴＫ２）を生成する（ステップＳ１６１１）。そして、ＴＫＦ回復部１４３は、新たな乱数２（ＢＮ２）と、新たなＴＫＦ乱数２（ＴＫＦＮ２）と更新された世代と生成された暗号化タイトルキー（ＥＴＫ２）とからバックアップファイルＴＫＦ＃２を生成し（ステップＳ１６１２）、ＴＫＦ＃２を回復する。回復されたバックアップファイルＴＫＦ＃２は、ＴＫＦ回復部１４３からドライブ部１１０に送られて記録部１１３によって乱数２（ＢＮ２）とともにＤＶＤメディア１４０に記録する（ステップＳ１６１３）。
【０１０７】
次に、ＴＫＦ回復部１４３はドライブ部１１０に乱数生成を要求して、乱数生成部１１１によって再生成された新たな乱数３（ＢＮ３）をドライブ部１１０から取得する（ステップＳ１６１４）。そして、ＴＫＦ回復部１４３は、新たな乱数３（ＢＮ３）と、新たなＴＫＦ乱数１（ＴＫＦＮ１）と、新たなＴＫＦ乱数２（ＴＫＦＮ２）と、更新された世代とから、図１２に示す構造のバックアップファイルＴＫＦ＃３を生成し（ステップＳ１６１５）、ＴＫＦ＃３を回復する。回復されたバックアップファイルＴＫＦ＃３は、ＴＫＦ回復部１４３からドライブ部１１０に送られて記録部１１３によって乱数３（ＢＮ３）とともにＤＶＤメディア１４０に記録する（ステップＳ１６１６）。このようにして、ＴＫＦ＃２およびＴＫＦ＃３を用いて全てのバックアップファイルが回復されることになる。
【０１０８】
次に、タイトルキーファイルＴＫＦ＃１およびバックアップファイルＴＫＦ＃３の回復処理について説明する。図１７は、タイトルキーファイルＴＫＦ＃１、バックアップファイル＃３による回復処理の手順を示すフローチャートである。本実施の形態では、バックアップファイルＴＫＦ＃１の暗号化タイトルキー（ＥＴＫ１）の復号処理、タイトルキーファイルＴＫＦ＃１の暗号化タイトルキー（ＥＴＫ１）の生成処理、タイトルキーファイルＴＫＦ＃１の生成処理、バックアップファイルＴＫＦ＃３の生成処理が、図９で説エニした実施の形態１におけるＴＫＦ＃１による回復処理と異なっている。
【０１０９】
まず、ＴＫＦ回復部１４３は、ＴＫＦ＃３の乱数３（ＢＮ３）が格納されるプロテクト領域に不当情報としての０が設定されているか否かを調べる（ステップＳ１６０１）。そして、ＴＫＦ＃３の乱数３（ＢＮ３）に０が設定されている場合には（ステップＳ１７０１：Ｙｅｓ）、例えば、エディタなどのアプリケーションによりＴＫＦ＃３のユーザ領域にあるＴＫＦＮ１，ＴＫＦＮ２の値が変更され、不当な更新である場合があるので、エラー処理を行って（ステップＳ１７１７）、回復処理を行わずに終了する。
【０１１０】

一方、ステップＳ１７０１において、ＴＫＦ＃３の乱数３（ＢＮ３）が格納されるプロテクト領域に０が設定されていない場合には（ステップＳ１７０１：Ｎｏ）、ＴＫＦ＃３は正当なものであると判断して、以下の回復処理を続行する。

【０１１１】

ＴＫＦ回復部１４３は、ドライブ部１１０からＤＶＤメディア１４０上に記録された乱数１（ＢＮ１）とＴＫＦ＃１，ＴＫＦ＃３を取得する（ステップＳ１７０２）。そして、バックアップファイルＴＫＦ＃１の暗号化タイトルキー（ＥＴＫ１）を、乱数１（ＢＮ１）と、ＴＫＦ＃３に格納されているＴＫＦ乱数２（ＴＫＦＮ２）とによって（４）式によって復号化し（ステップＳ１７０３）、タイトルキー（ＴＫ）を得る。そして、ＴＫＦ更新部１４２は、ＴＫＦ乱数１、２（ＴＫＦＮ１，ＴＫＦＮ２）を新たに乱数生成し（ステップＳ１７０４）、世代を１増加して更新する（ステップＳ１７０５）。

【０１１２】

これ以降のステップＳ１７０６からＳ１７１６までのＴＫＦ＃１、ＴＫＦ＃２、ＴＫＦ＃３の回復処理は、図１６のステップＳ１６０６からＳ１６１６までの処理と同様に行われる。このようにして、ＴＫＦ＃１およびＴＫＦ＃３を用いて全てのバックアップファイルが回復されることになる。

【０１１３】

次に、タイトルキーファイルＴＫＦ＃１、バックアップファイル＃２による回復処理について説明する。図１８は、タイトルキーファイルＴＫＦ＃１、バックアップファイルＴＫＦ＃２による回復処理の手順を示すフローチャートである。ＴＫＦ回復部１４３は、ＴＫＦ＃３が存在しない場合か破壊されている場合、もしくはＴＫＦ＃３の世代がＴＫＦ＃２およびＴＫＦ＃１の世代より小さい場合には、ＴＫＦ＃１およびＴＫＦ＃２を用いてＴＫＦ＃３の回復処理を行う。

【０１１４】

このため、まず、ＴＫＦ回復部１４３は、ＴＫＦ＃１の乱数１（ＢＮ１）およびＴＫＦ＃２の乱数２（ＢＮ２）に不当情報としての０が設定されているか否かを調べる（ステップＳ１８０１）。そして、ＴＫＦ＃１の乱数１（ＢＮ１）およびＴＫＦ＃２の乱数２（ＢＮ２）に０が設定されている場合には（ステップＳ１８０１：Ｙｅｓ）、例えば、エディタなどのアプリケーションによりタイトルキーファイルＴＫＦ＃１のユーザ領域にあるＴＫＦＮ２またはバックアップファイルＴＫＦ＃２のユーザ領域にあるＴＫＦＮ１の値が変更され、不当な更新である場合があるので、エラー処理を行って（ステップＳ１８０５）、回復処理を行わずに終了する。

【０１１５】

一方、ステップＳ１８０１において、ＴＫＦ＃１の乱数１（ＢＮ１）およびＴＫＦ＃２の乱数２（ＢＮ２）に０が設定されていない場合には（ステップＳ１８０１：Ｎｏ）、ＴＫＦは正当なものであると判断して、以下の回復処理を続行する。

【０１１６】

ＴＫＦ回復部１４３は、ドライブ部１１０からメディア上に記録された乱数（ＢＮ３）とＴＫＦ＃１，ＴＫＦ＃２を取得する（ステップＳ１８０２）。そしてＴＫＦ＃１からＴＫＦ乱数１（ＴＫＦＮ１）と世代を、ＴＫＦ＃２からＴＫＦ乱数２（ＴＫＦＮ２）と世代を読み出し、新たな乱数３（ＢＮ３）と世代とＴＫＦ乱数１（ＴＫＦＮ１）とＴＫＦ乱数２（ＴＫＦＮ２）とから、図１２に示す構造のバックアップファイルＴＫＦ＃３を生成し（ステップＳ１８０３）、ＴＫＦ＃３を回復する。回復されたバックアップファイルＴＫＦ＃３は、ＴＫＦ回復部１４３からドライブ部１１０に送られて記録部１１３によって乱数３（ＢＮ３）とともにＤＶＤメディア１４０に記録する（ステップＳ１８０４）。このようにして、ＴＫＦ＃１、ＴＫＦ＃２を用いてＴＫＦ＃３のバックアップファイルが回復されることになる。

【０１１７】

このように、実施の形態２にでは、タイトルキー（ＴＫ）の暗号化ファイルをＴＫＦ＃１、ＴＫＦ＃２の２つ用意し、ＴＫＦ＃３を乱数３とＴＫＦ乱数２とＴＫＦ乱数３と世代

とで構成し、ＴＫＦ＃１、ＴＫＦ＃２の暗号化タイトルキーを、自己の乱数と互いのＴＫＦ乱数によって（４）、（５）のように暗号化している。このため、実施の形態１と同様に、ＤＶＤメディアから削除したタイトルコンテンツに対するタイトルキーを不正に復元されてしまうことを防止し、タイトルコンテンツの不正な利用を防止することができる。

【０１１８】

（変形例２）

上述した実施の形態１および２のコンテンツ記録再生装置１００において、ドライブ部１１０とホスト部１２０がバス３０にて接続された構成について説明してきたが、ドライブ部１１０とホスト部１２０が内部バスで接続され、一体で構成することもできる。図１９は、ドライブ部１１０とホスト部１２０が内部バス１９３０で接続され、一体構成されたコンテンツ記録再生装置１９００の構成を示すブロック図である。

【０１１９】

図１９に示すように、ドライブ部１１０に含まれる各部は、実施の形態と同様のであるが、ホスト部１９２０では、乱数生成部を備えていない。図１９の構成では、ドライブ部１１０内の乱数生成部１１１が、ホスト部１９２０およびドライブ部１１０から共用で利用されるようになっている。

【０１２０】

なお、図１９では乱数生成部１１１がドライブ部１１０に含まれる構成を採用しているが、この他、ドライブ部１１０には乱数生成部が含まれず、ホスト部１９２０にのみ備えたり、ドライブ部１１０とホスト部１９２０には直接含まれず、装置内の別の処理部に備えるように構成してもよい。

【０１２１】

なお、実施の形態１および２のコンテンツ記録再生装置で実行されるコンテンツ記録再生プログラムは、ＲＯＭ等に予め組み込まれて提供される。

【０１２２】

実施の形態１および２のコンテンツ記録再生装置で実行されるコンテンツ記録再生プログラムは、インストール可能な形式又は実行可能な形式のファイルでＣＤ－ＲＯＭ、フレキシブルディスク（ＦＤ）、ＣＤ－Ｒ、ＤＶＤ等のコンピュータで読み取り可能な記録媒体に記録して提供するように構成してもよい。

【０１２３】

さらに、実施の形態１および２のコンテンツ記録再生装置で実行されるコンテンツ記録再生プログラムを、インターネット等のネットワークに接続されたコンピュータ上に格納し、ネットワーク経由でダウンロードさせることにより提供するように構成しても良い。また、実施の形態１および２のコンテンツ記録再生装置で実行されるコンテンツ記録再生プログラムをインターネット等のネットワーク経由で提供または配布するように構成しても良い。

【０１２４】

実施の形態１および２のコンテンツ記録再生装置で実行されるコンテンツ記録再生プログラムは、上述した各部（コンテンツ暗号化処理部１２１、コンテンツ復号化処理部１２２、ＴＫＦ暗号化処理部１２３、バックアップ処理部１４０）を含むモジュール構成となっており、実際のハードウェアとしてはＣＰＵ（プロセッサ）が上記ＲＯＭからコンテンツ記録再生プログラムを読み出して実行することにより上記各部が主記憶装置上にロードされ、コンテンツ暗号化処理部１２１、コンテンツ復号化処理部１２２、ＴＫＦ暗号化処理部１２３、バックアップ処理部１４０が主記憶装置上に生成されるようになっている。

【０１２５】

なお、実施の形態１および２のコンテンツ記録再生装置は、ＤＶＤレコーダのような組み込み機器ではなく、ＣＰＵなどの制御装置と、ＲＯＭ（Read Only Memory）やＲＡＭなどの記憶装置と、ＨＤＤ、ＣＤドライブ装置などの外部記憶装置と、ディスプレイ装置などの表示装置と、キーボードやマウスなどの入力装置を備えており、通常のコンピュータを利用した構成とすることもできる。この場合に、ホスト部１２０とドライブ部１１０と

を繋ぐバスは、例えば、ＵＳＢ等を利用することができる。

【０１２６】

なお、本発明は、上記実施の形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化することができる。

【図面の簡単な説明】

【０１２７】

【図１】実施の形態１にかかるコンテンツ記録再生装置１００の構成を示すブロック図である。

【図２】セクタの構造を示す説明図である。

【図３】乱数をＤＶＤメディア１４０に書き込む処理の手順を示すシーケンス図である。

【図４－１】実施の形態１のタイトルキーファイルとバックアップファイルの構造を示す説明図である。

【図４－２】暗号化キーファイルのデータ構造を示す説明図である。

【図５】タイトルキーファイル（ＴＫＦ）のバックアップの初期化処理の手順を示すフローチャートである。

【図６－１】タイトルキーファイル（ＴＫＦ）のバックアップの更新処理の手順を示すフローチャートである。

【図６－２】タイトルキーファイルＴＫＦ＃１を復号し、再生成した乱数１にて暗号化した後、ＴＫＦ＃１と再生成した乱数１をＤＶＤメディア１４０に書き込む処理の手順を示したシーケンス図である。

【図７】タイトルキーファイル（ＴＫＦ）のバックアップの回復の全体処理の手順を示すフローチャートである。

【図８】バックアップファイルＴＫＦ＃３による回復処理の手順を示すフローチャートである。

【図９】バックアップファイルＴＫＦ＃１による回復処理の手順を示すフローチャートである。

【図１０】バックアップファイルＴＫＦ＃２による回復処理の手順を示すフローチャートである。

【図１１】世代を更新処理時に毎回乱数生成した場合におけるタイトルキーファイル（ＴＫＦ）のバックアップの回復処理の全体処理の手順を示すフローチャートである。

【図１２】実施の形態２のタイトルキーファイルとバックアップファイルの構造を示す説明図である。

【図１３】タイトルキーファイル（ＴＫＦ）のバックアップの初期化処理の手順を示すフローチャートである。

【図１４】実施の形態２におけるタイトルキーファイル（ＴＫＦ）のバックアップの更新処理の手順を示すフローチャートである。

【図１５】実施の形態２におけるタイトルキーファイル（ＴＫＦ＃１）のバックアップの回復の全体処理の手順を示すフローチャートである。

【図１６】実施の形態２におけるバックアップファイルＴＫＦ＃２、＃３による回復処理の手順を示すフローチャートである。

【図１７】実施の形態２におけるタイトルキーファイルＴＫＦ＃１、バックアップファイル＃３による回復処理の手順を示すフローチャートである。

【図１８】実施の形態２におけるタイトルキーファイルＴＫＦ＃１、バックアップファイルＴＫＦ＃２による回復処理の手順を示すフローチャートである。

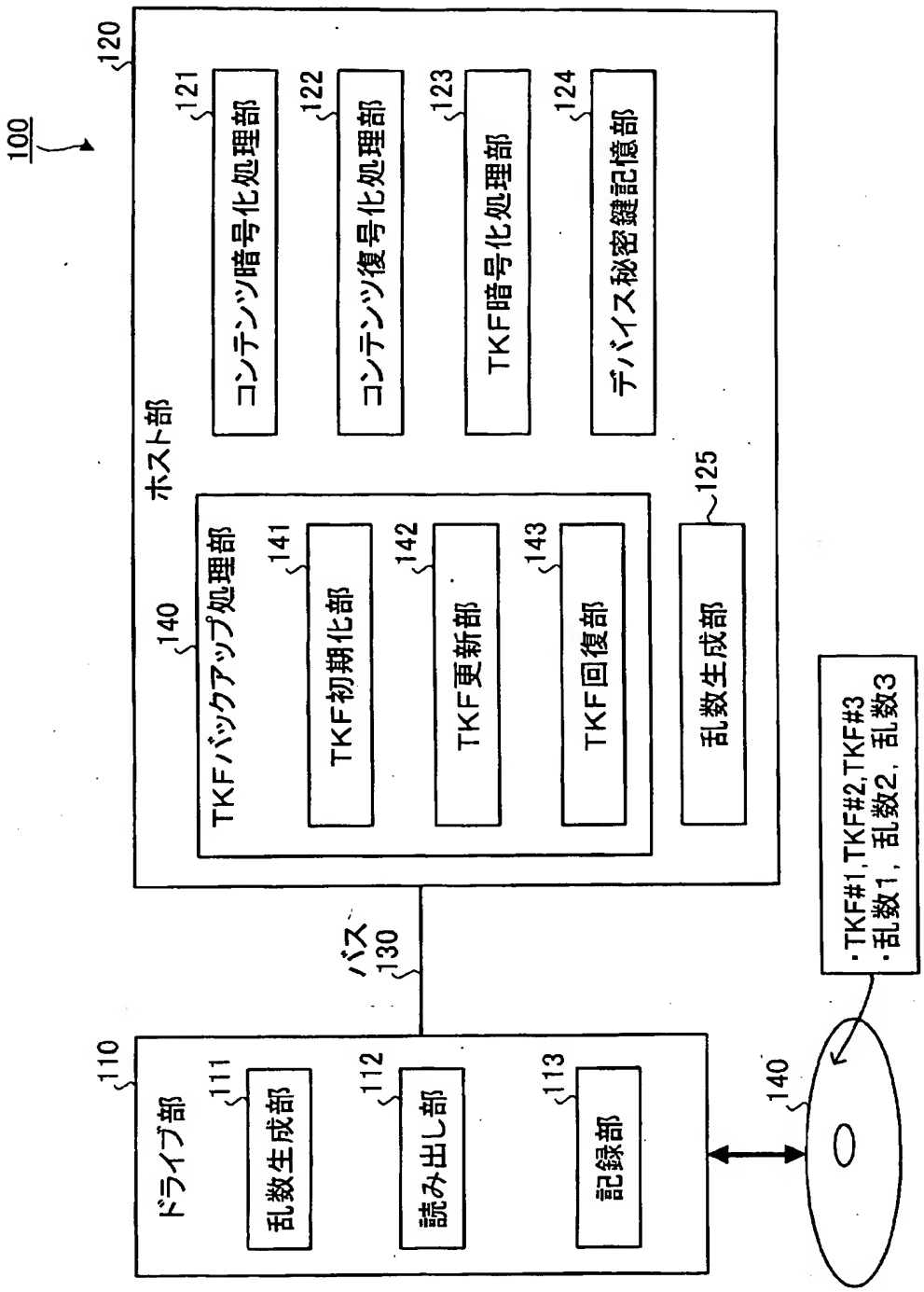
【図１９】ドライブ部１１０とホスト部１２０が内部バスで接続され、一体構成されたコンテンツ記録再生装置１９００の構成を示すブロック図である。

【符号の説明】

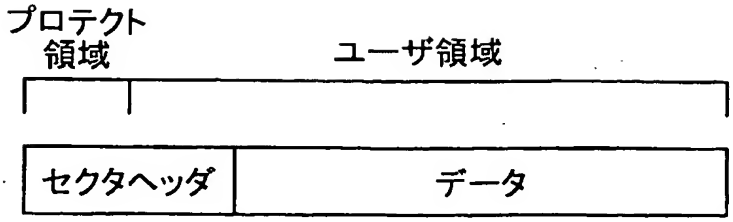
【０１２８】

１００　コンテンツ記録再生装置
１１０　ドライブ部
１１１　乱数生成部
１１２　読み出し部
１１３　記録部
１２０　ホスト部
１２１　コンテンツ暗号化処理部
１２２　コンテンツ復号化処理部
１２３　ＴＫＦ暗号化処理部
１２４　デバイス秘密鍵記憶部
１２５　乱数生成部
１３０　バス
１４０　ＤＶＤメディア

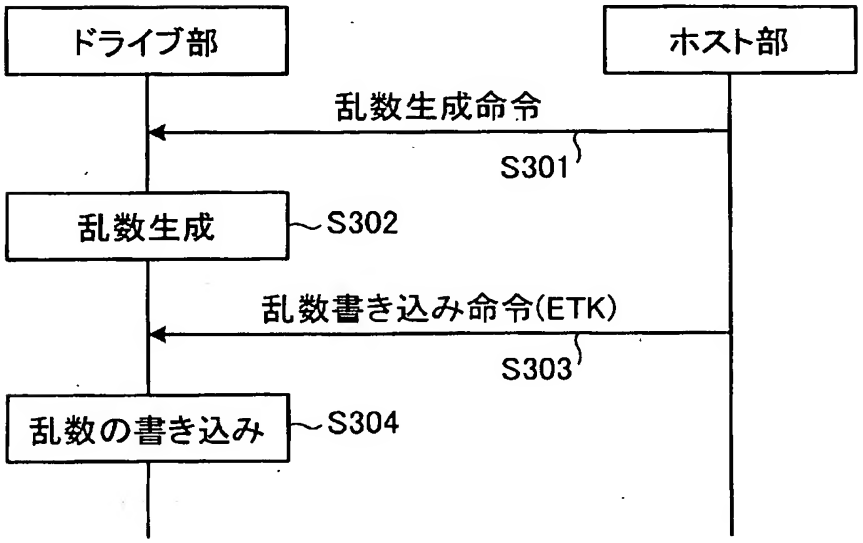
【書類名】図面
【図１】


100
120
ホスト部
121
コンテンツ暗号化処理部
122
コンテンツ復号化処理部
123
TKF暗号化処理部
124
デバイス秘密鍵記憶部
TKFバックアップ処理部
140
141
TKF初期化部
142
TKF更新部
143
TKF回復部
125
乱数生成部
バス
130
110
ドライブ部
111
乱数生成部
112
読み出し部
113
記録部
140
・TKF#1,TKF#2,TKF#3
・乱数1，乱数2，乱数3

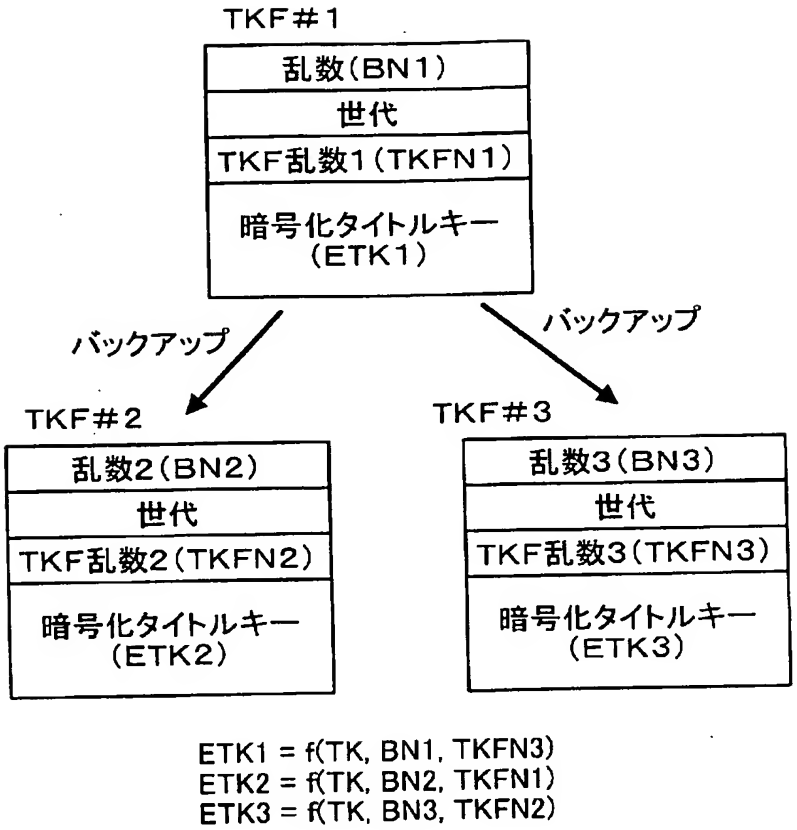
【図２】


プロテクト
領域
ユーザ領域
セクタヘッダ
データ

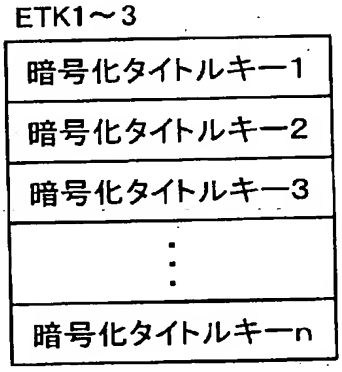
【図３】


ドライブ部
ホスト部
乱数生成命令
S301
乱数生成
S302
乱数書き込み命令(ETK)
S303
乱数の書き込み
S304

【図４－１】


TKF＃1
乱数(BN1)
世代
TKF乱数1(TKFN1)
暗号化タイトルキー
(ETK1)
バックアップ
バックアップ
TKF＃2
乱数2(BN2)
世代
TKF乱数2(TKFN2)
暗号化タイトルキー
(ETK2)
TKF＃3
乱数3(BN3)
世代
TKF乱数3(TKFN3)
暗号化タイトルキー
(ETK3)
ETK1 = f(TK, BN1, TKFN3)
ETK2 = f(TK, BN2, TKFN1)
ETK3 = f(TK, BN3, TKFN2)

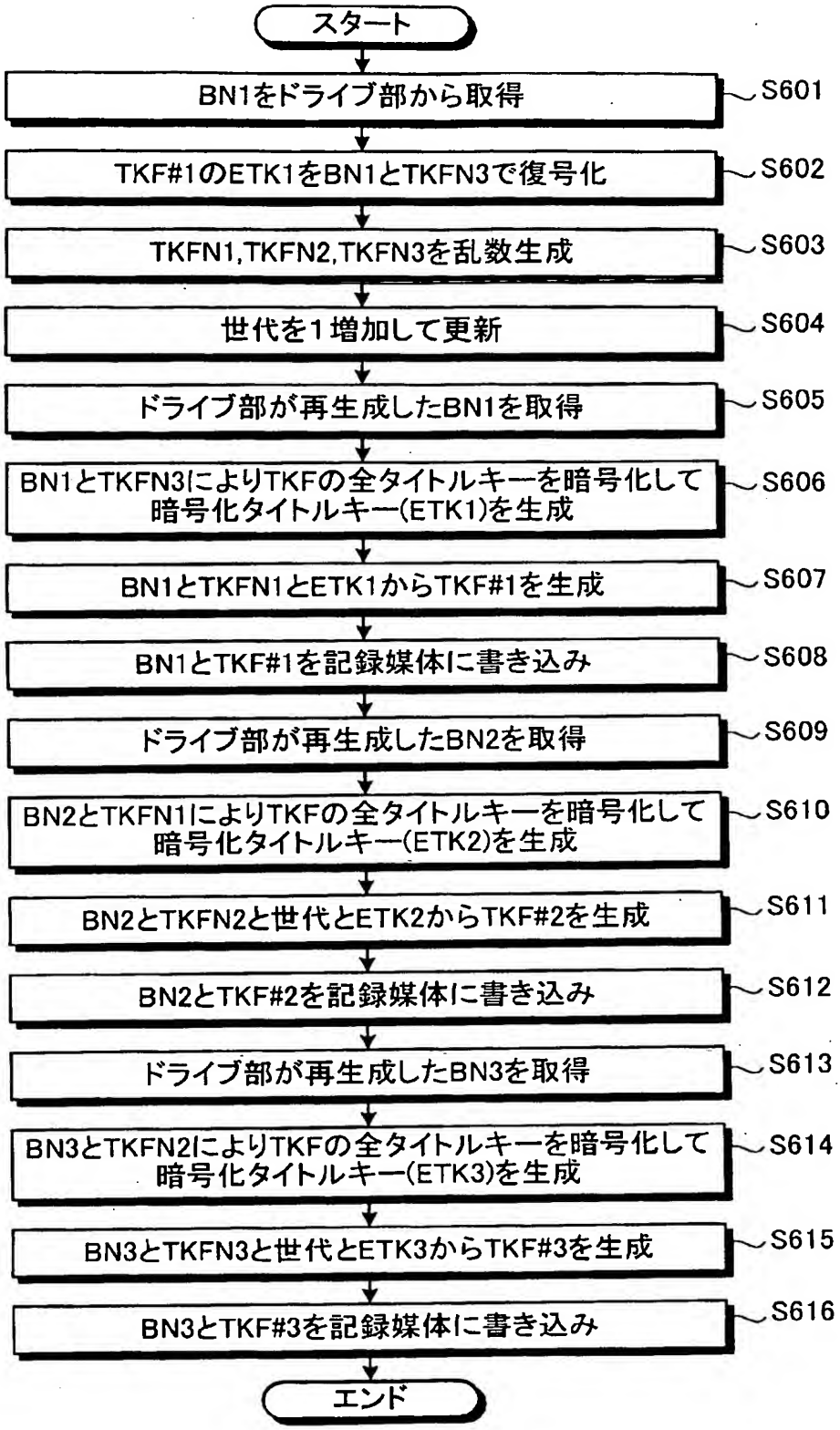
【図４－２】


ETK1～3
暗号化タイトルキー1
暗号化タイトルキー2
暗号化タイトルキー3
暗号化タイトルキーn

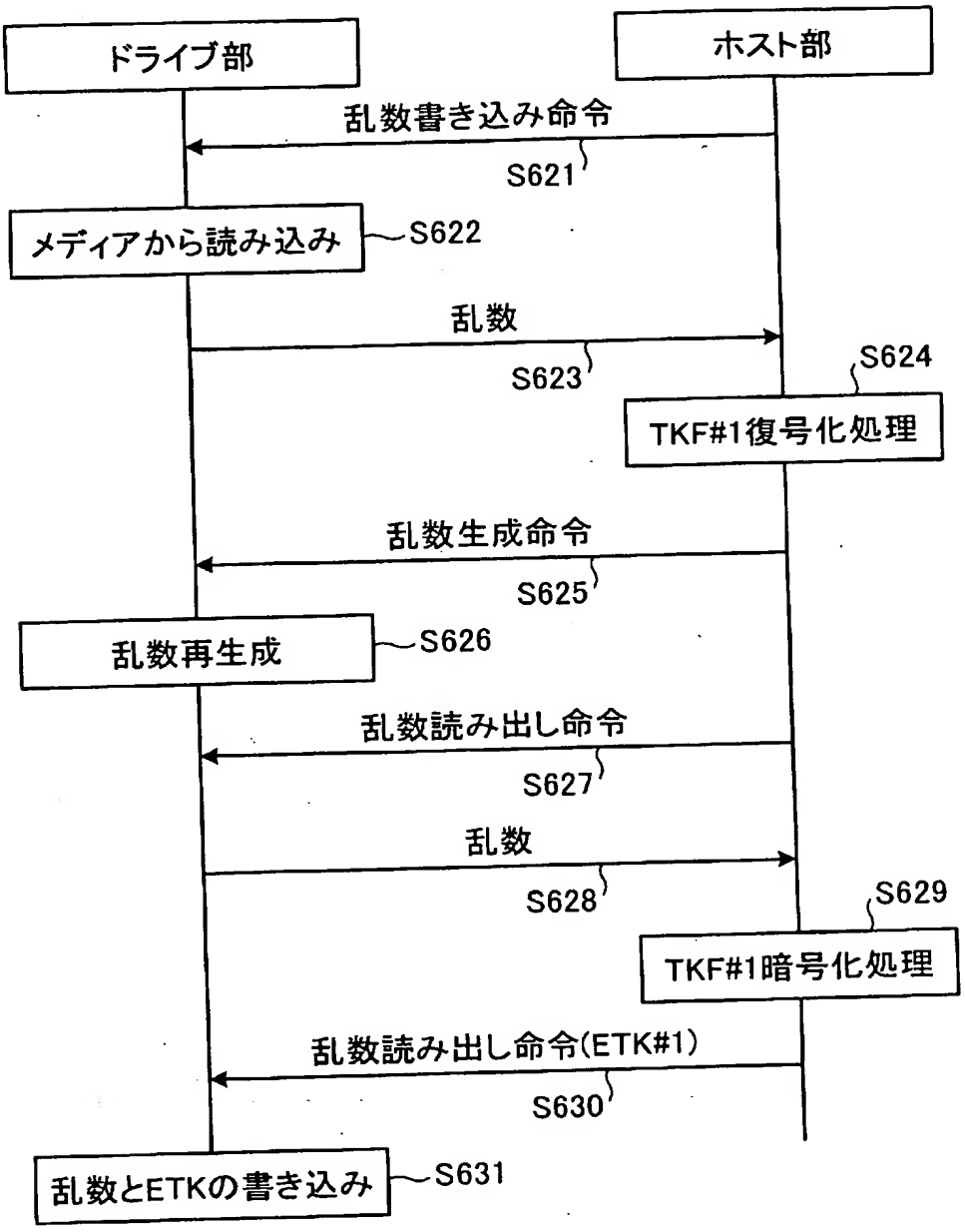
【図５】


スタート
TKF1，TKF2，TKF3を乱数生成
S501
世代を乱数生成
S502
ドライブ部から乱数1(BN1)を取得
S503
BN1とTKFN3からTKFの全タイトルキーを暗号化して暗号化タイトルキー(ETK1)を生成
S504
BN1とTKFN1と世代とETK1からTKF#1を生成
S505
BN1とTKF#1を記録媒体に書き込み
S506
ドライブ部から乱数2(BN2)を取得
S507
BN2とTKFN1からTKFの全タイトルキーを暗号化して暗号化タイトルキー(ETK2)を生成
S508
BN2とTKFN2と世代とETK2からTKF#2を生成
S509
BN2とTKF#2を記録媒体に書き込み
S510
ドライブ部から乱数3(BN3)を取得
S511
BN3とTKFN2からTKFの全タイトルキーを暗号化して暗号化タイトルキー(ETK3)を生成
S512
BN3とTKFN3と世代とETK3からTKF#3を生成
S513
BN3とTKF#3を記録媒体に書き込み
S514
エンド

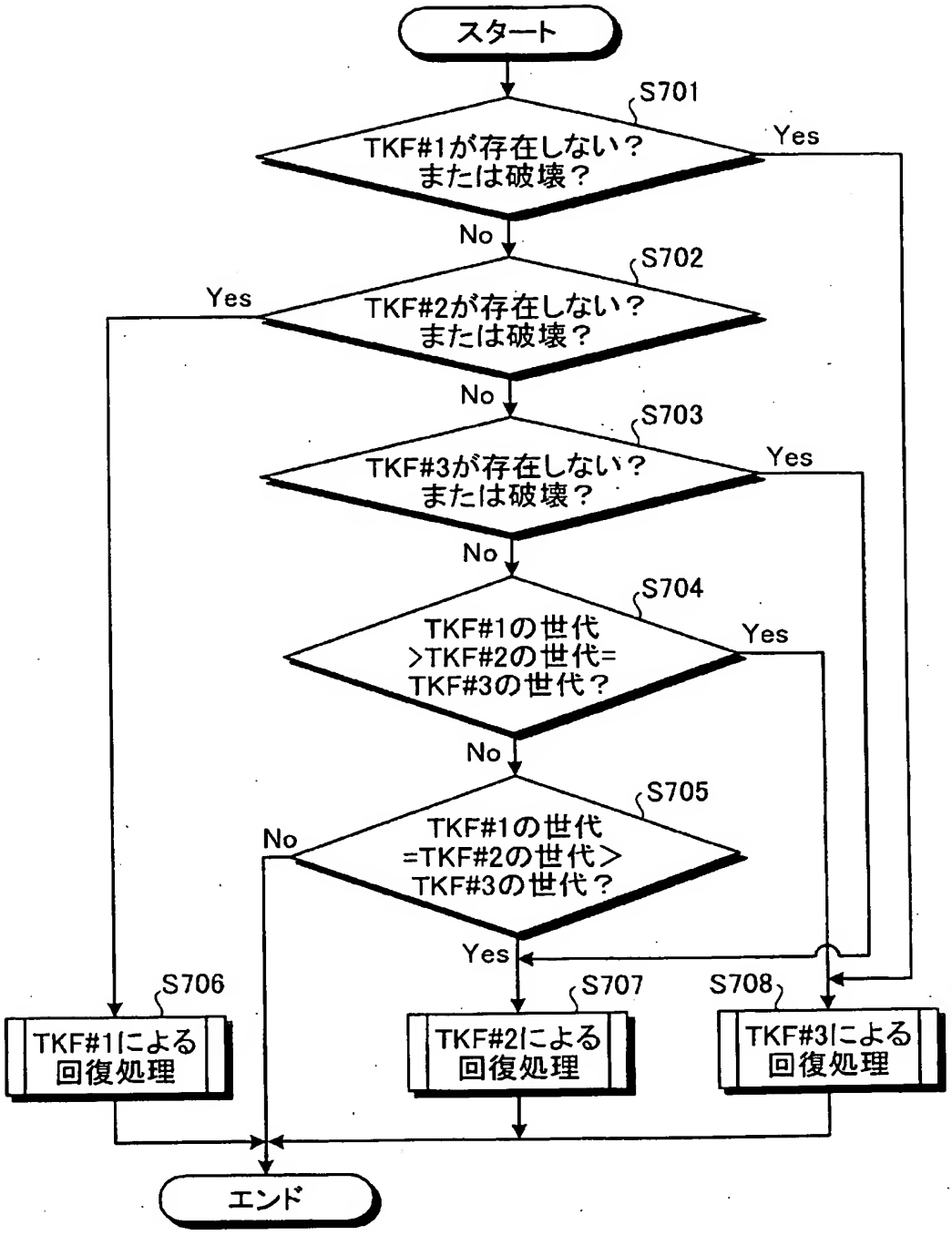
【図６－１】


スタート
BN1をドライブ部から取得
S601
TKF#1のETK1をBN1とTKFN3で復号化
S602
TKFN1,TKFN2,TKFN3を乱数生成
S603
世代を1増加して更新
S604
ドライブ部が再生成したBN1を取得
S605
BN1とTKFN3によりTKFの全タイトルキーを暗号化して
暗号化タイトルキー(ETK1)を生成
S606
BN1とTKFN1とETK1からTKF#1を生成
S607
BN1とTKF#1を記録媒体に書き込み
S608
ドライブ部が再生成したBN2を取得
S609
BN2とTKFN1によりTKFの全タイトルキーを暗号化して
暗号化タイトルキー(ETK2)を生成
S610
BN2とTKFN2と世代とETK2からTKF#2を生成
S611
BN2とTKF#2を記録媒体に書き込み
S612
ドライブ部が再生成したBN3を取得
S613
BN3とTKFN2によりTKFの全タイトルキーを暗号化して
暗号化タイトルキー(ETK3)を生成
S614
BN3とTKFN3と世代とETK3からTKF#3を生成
S615
BN3とTKF#3を記録媒体に書き込み
S616
エンド

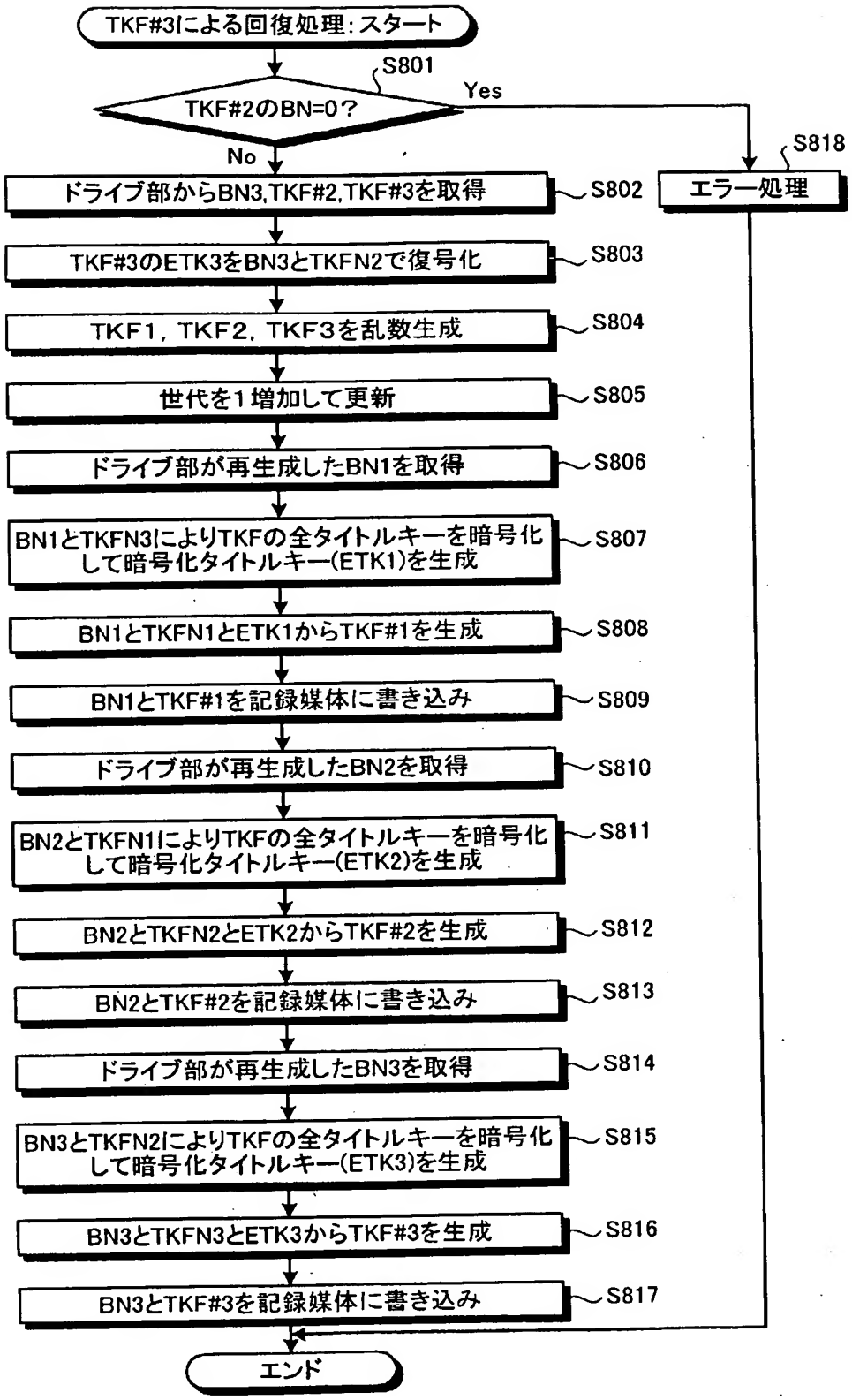
【図６－２】


ドライブ部
ホスト部
乱数書き込み命令
S621
メディアから読み込み
S622
乱数
S623
S624
TKF#1復号化処理
乱数生成命令
S625
乱数再生成
S626
乱数読み出し命令
S627
乱数
S628
S629
TKF#1暗号化処理
乱数読み出し命令(ETK#1)
S630
乱数とETKの書き込み
S631

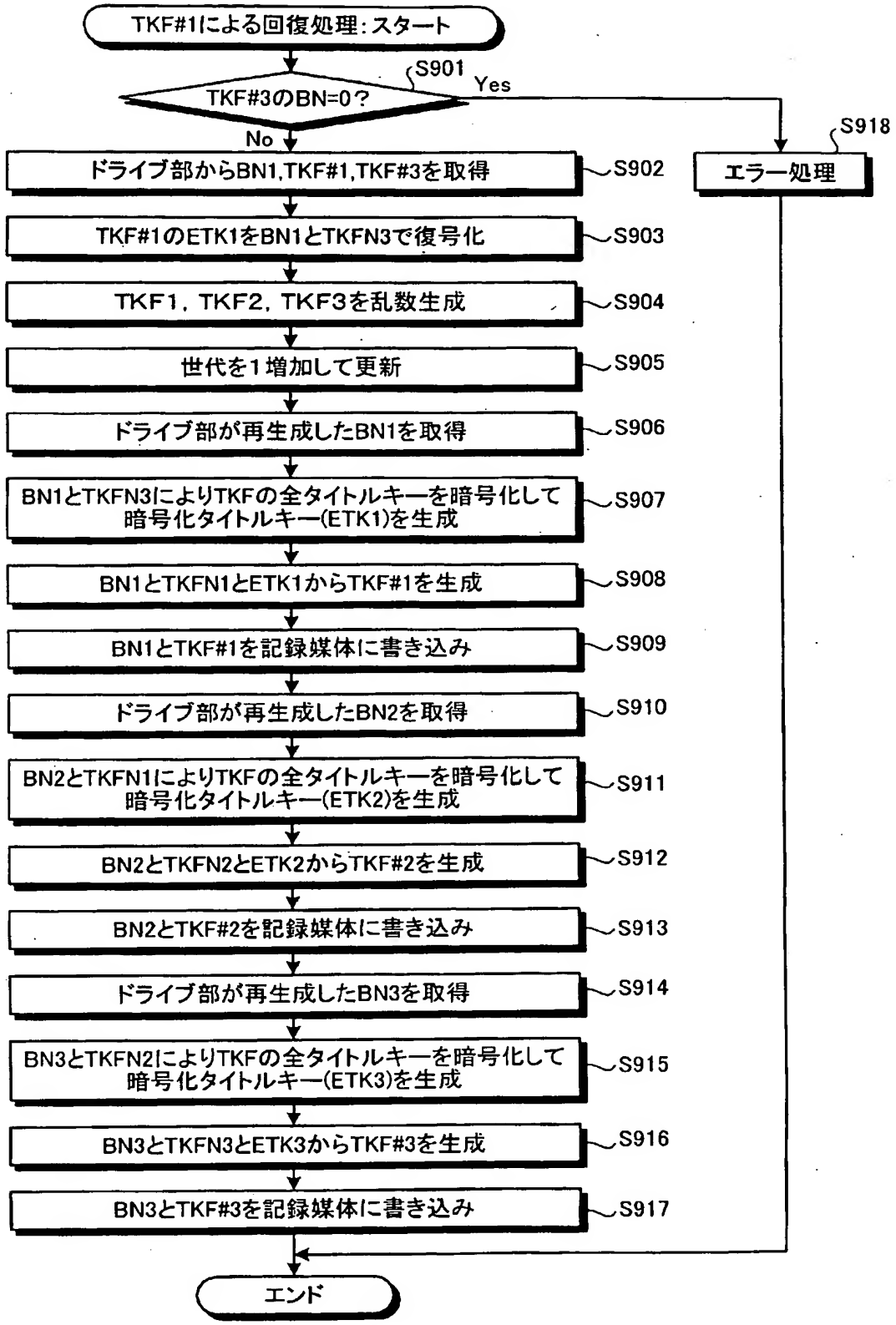
【図７】


スタート
S701
TKF#1が存在しない？
または破壊？
Yes
No
S702
TKF#2が存在しない？
または破壊？
Yes
No
S703
TKF#3が存在しない？
または破壊？
Yes
No
S704
TKF#1の世代
>TKF#2の世代=
TKF#3の世代？
Yes
No
S705
TKF#1の世代
=TKF#2の世代>
TKF#3の世代？
No
Yes
S706
TKF#1による
回復処理
S707
TKF#2による
回復処理
S708
TKF#3による
回復処理
エンド

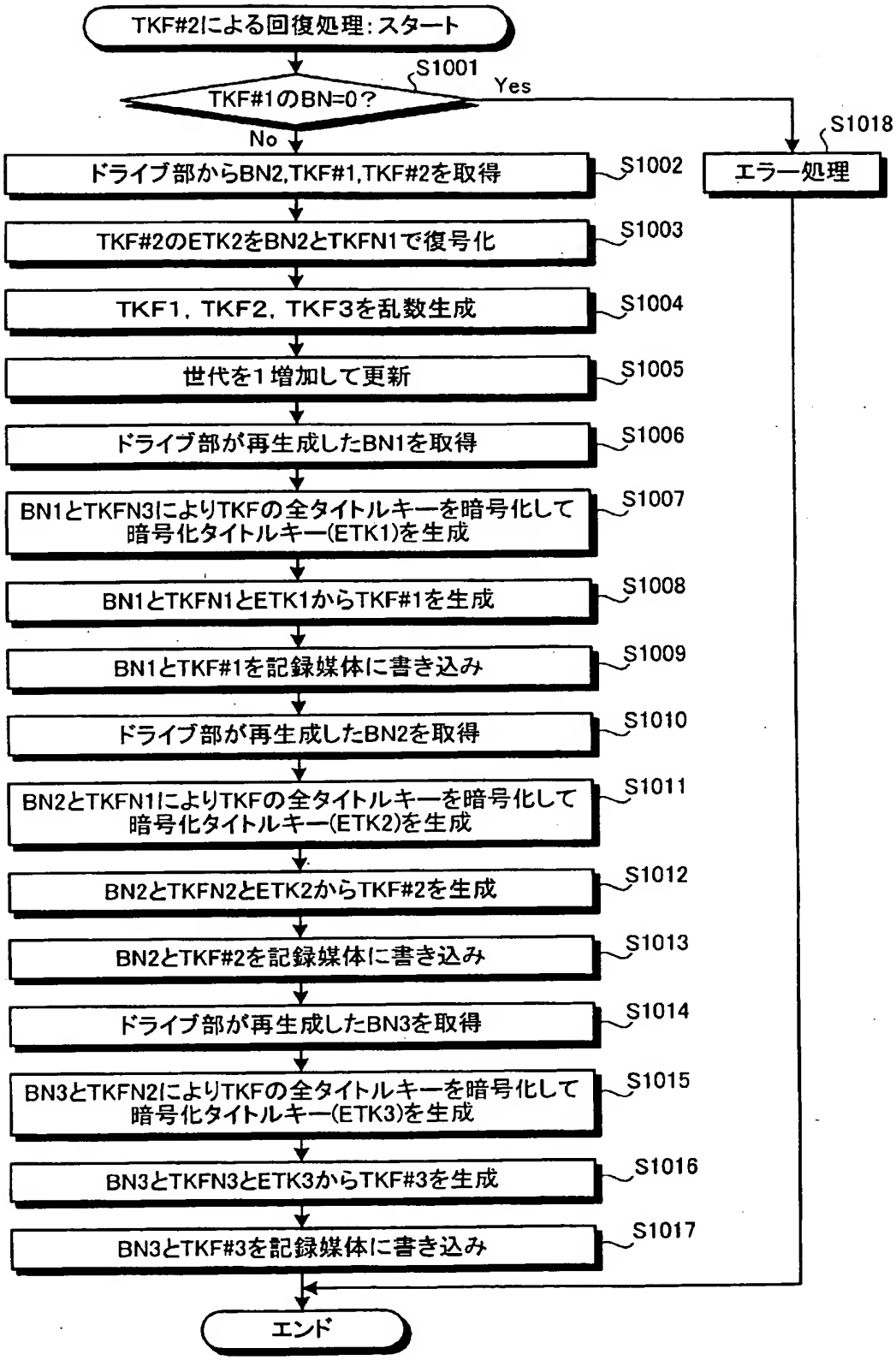
【図８】


TKF#3による回復処理：スタート
S801
TKF#2のBN=0？
Yes
No
S818
エラー処理
ドライブ部からBN3,TKF#2,TKF#3を取得
S802
TKF#3のETK3をBN3とTKFN2で復号化
S803
TKF1，TKF2，TKF3を乱数生成
S804
世代を1増加して更新
S805
ドライブ部が再生成したBN1を取得
S806
BN1とTKFN3によりTKFの全タイトルキーを暗号化して暗号化タイトルキー(ETK1)を生成
S807
BN1とTKFN1とETK1からTKF#1を生成
S808
BN1とTKF#1を記録媒体に書き込み
S809
ドライブ部が再生成したBN2を取得
S810
BN2とTKFN1によりTKFの全タイトルキーを暗号化して暗号化タイトルキー(ETK2)を生成
S811
BN2とTKFN2とETK2からTKF#2を生成
S812
BN2とTKF#2を記録媒体に書き込み
S813
ドライブ部が再生成したBN3を取得
S814
BN3とTKFN2によりTKFの全タイトルキーを暗号化して暗号化タイトルキー(ETK3)を生成
S815
BN3とTKFN3とETK3からTKF#3を生成
S816
BN3とTKF#3を記録媒体に書き込み
S817
エンド

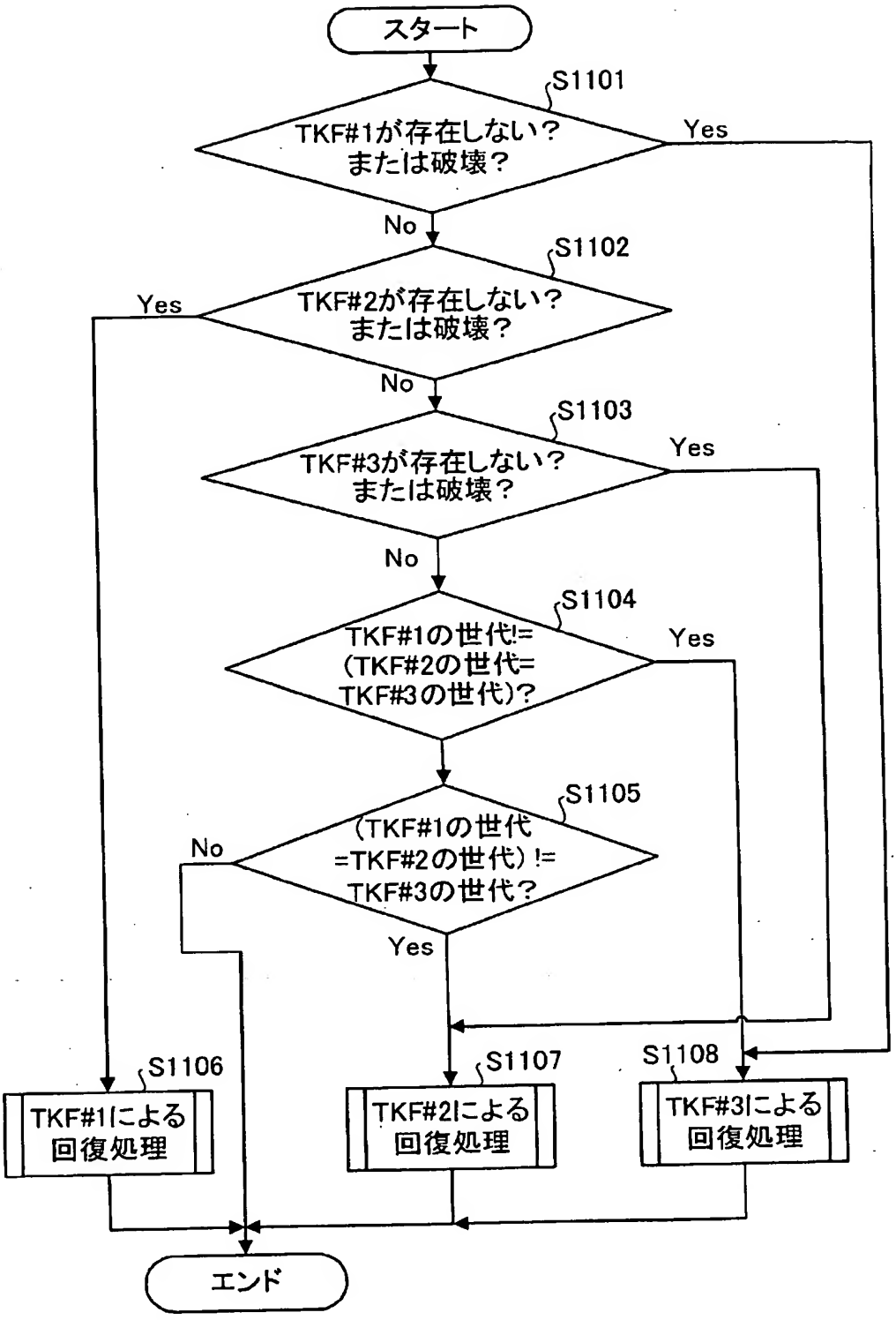
【図９】


TKF#1による回復処理：スタート
S901
TKF#3のBN=0？
Yes
No
S918
エラー処理
ドライブ部からBN1,TKF#1,TKF#3を取得
S902
TKF#1のETK1をBN1とTKFN3で復号化
S903
TKF1，TKF2，TKF3を乱数生成
S904
世代を1増加して更新
S905
ドライブ部が再生成したBN1を取得
S906
BN1とTKFN3によりTKFの全タイトルキーを暗号化して
暗号化タイトルキー(ETK1)を生成
S907
BN1とTKFN1とETK1からTKF#1を生成
S908
BN1とTKF#1を記録媒体に書き込み
S909
ドライブ部が再生成したBN2を取得
S910
BN2とTKFN1によりTKFの全タイトルキーを暗号化して
暗号化タイトルキー(ETK2)を生成
S911
BN2とTKFN2とETK2からTKF#2を生成
S912
BN2とTKF#2を記録媒体に書き込み
S913
ドライブ部が再生成したBN3を取得
S914
BN3とTKFN2によりTKFの全タイトルキーを暗号化して
暗号化タイトルキー(ETK3)を生成
S915
BN3とTKFN3とETK3からTKF#3を生成
S916
BN3とTKF#3を記録媒体に書き込み
S917
エンド

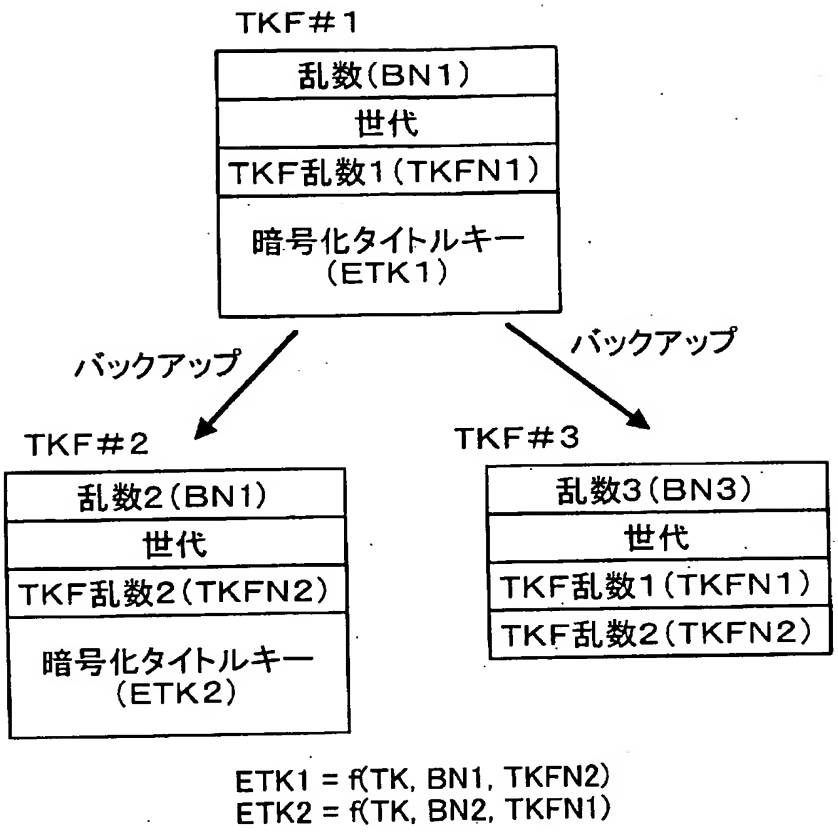
【図１０】


TKF#2による回復処理：スタート
S1001
TKF#1のBN=0？
Yes
No
S1018
エラー処理
ドライブ部からBN2,TKF#1,TKF#2を取得
S1002
TKF#2のETK2をBN2とTKFN1で復号化
S1003
TKF1，TKF2，TKF3を乱数生成
S1004
世代を1増加して更新
S1005
ドライブ部が再生成したBN1を取得
S1006
BN1とTKFN3によりTKFの全タイトルキーを暗号化して暗号化タイトルキー(ETK1)を生成
S1007
BN1とTKFN1とETK1からTKF#1を生成
S1008
BN1とTKF#1を記録媒体に書き込み
S1009
ドライブ部が再生成したBN2を取得
S1010
BN2とTKFN1によりTKFの全タイトルキーを暗号化して暗号化タイトルキー(ETK2)を生成
S1011
BN2とTKFN2とETK2からTKF#2を生成
S1012
BN2とTKF#2を記録媒体に書き込み
S1013
ドライブ部が再生成したBN3を取得
S1014
BN3とTKFN2によりTKFの全タイトルキーを暗号化して暗号化タイトルキー(ETK3)を生成
S1015
BN3とTKFN3とETK3からTKF#3を生成
S1016
BN3とTKF#3を記録媒体に書き込み
S1017
エンド

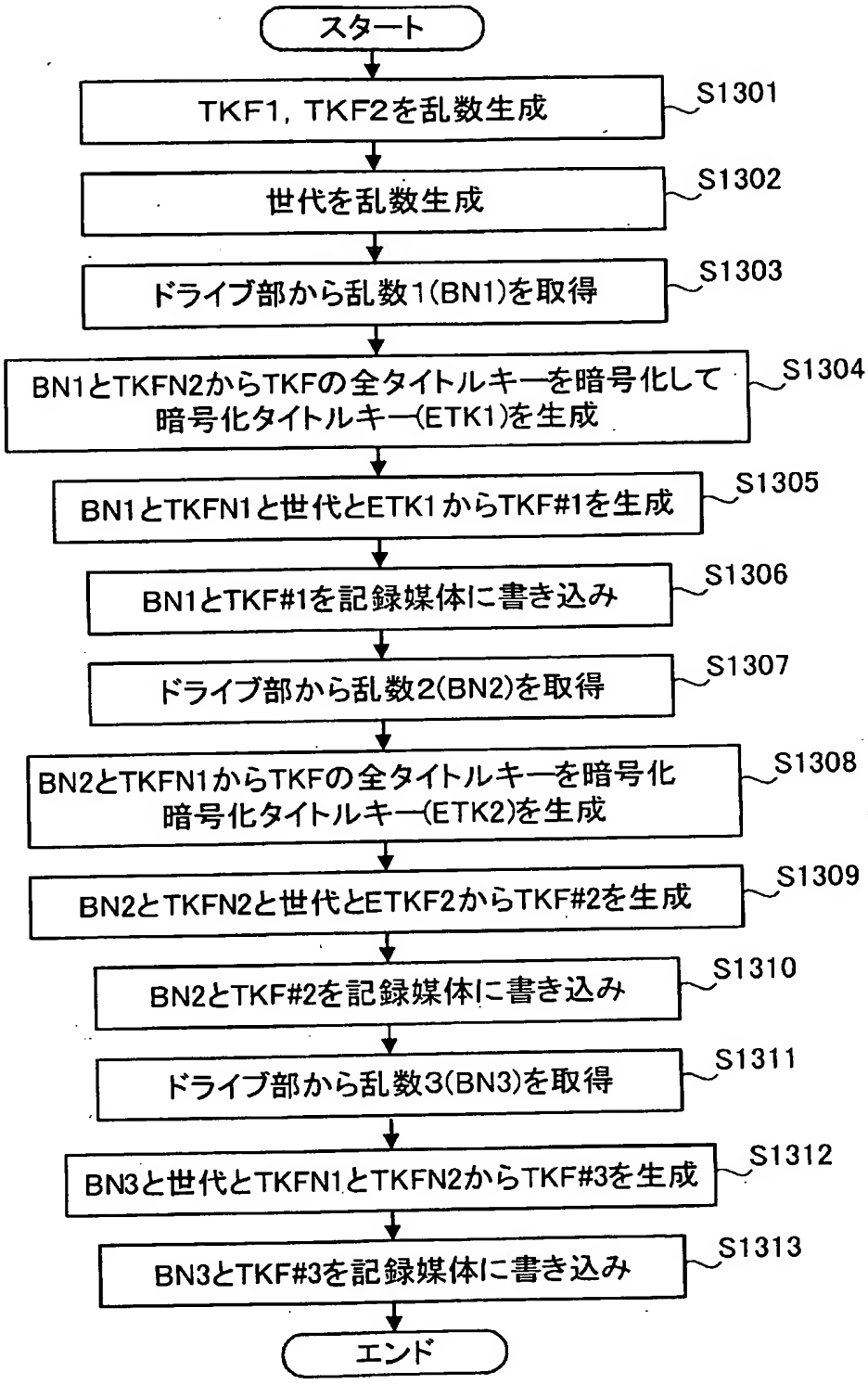
【図１１】


スタート
S1101
TKF#1が存在しない？
または破壊？
Yes
No
S1102
TKF#2が存在しない？
または破壊？
Yes
No
S1103
TKF#3が存在しない？
または破壊？
Yes
No
S1104
TKF#1の世代!=
(TKF#2の世代=
TKF#3の世代)？
Yes
S1105
(TKF#1の世代
=TKF#2の世代) !=
TKF#3の世代？
No
Yes
S1106
TKF#1による
回復処理
S1107
TKF#2による
回復処理
S1108
TKF#3による
回復処理
エンド

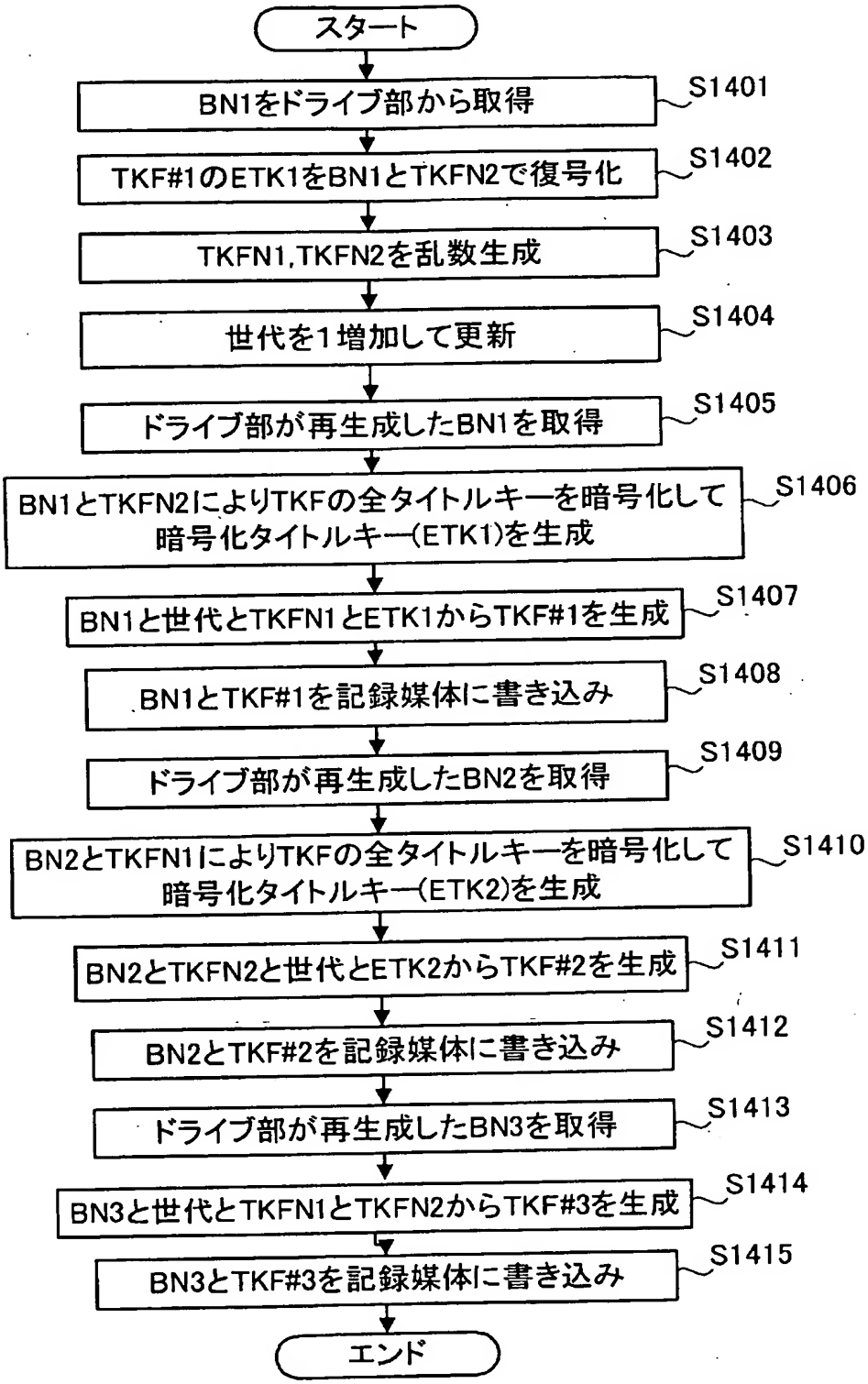
【図１２】


TKF#1
乱数(BN1)
世代
TKF乱数1(TKFN1)
暗号化タイトルキー
(ETK1)
バックアップ
バックアップ
TKF#2
乱数2(BN1)
世代
TKF乱数2(TKFN2)
暗号化タイトルキー
(ETK2)
TKF#3
乱数3(BN3)
世代
TKF乱数1(TKFN1)
TKF乱数2(TKFN2)
ETK1 = f(TK, BN1, TKFN2)
ETK2 = f(TK, BN2, TKFN1)

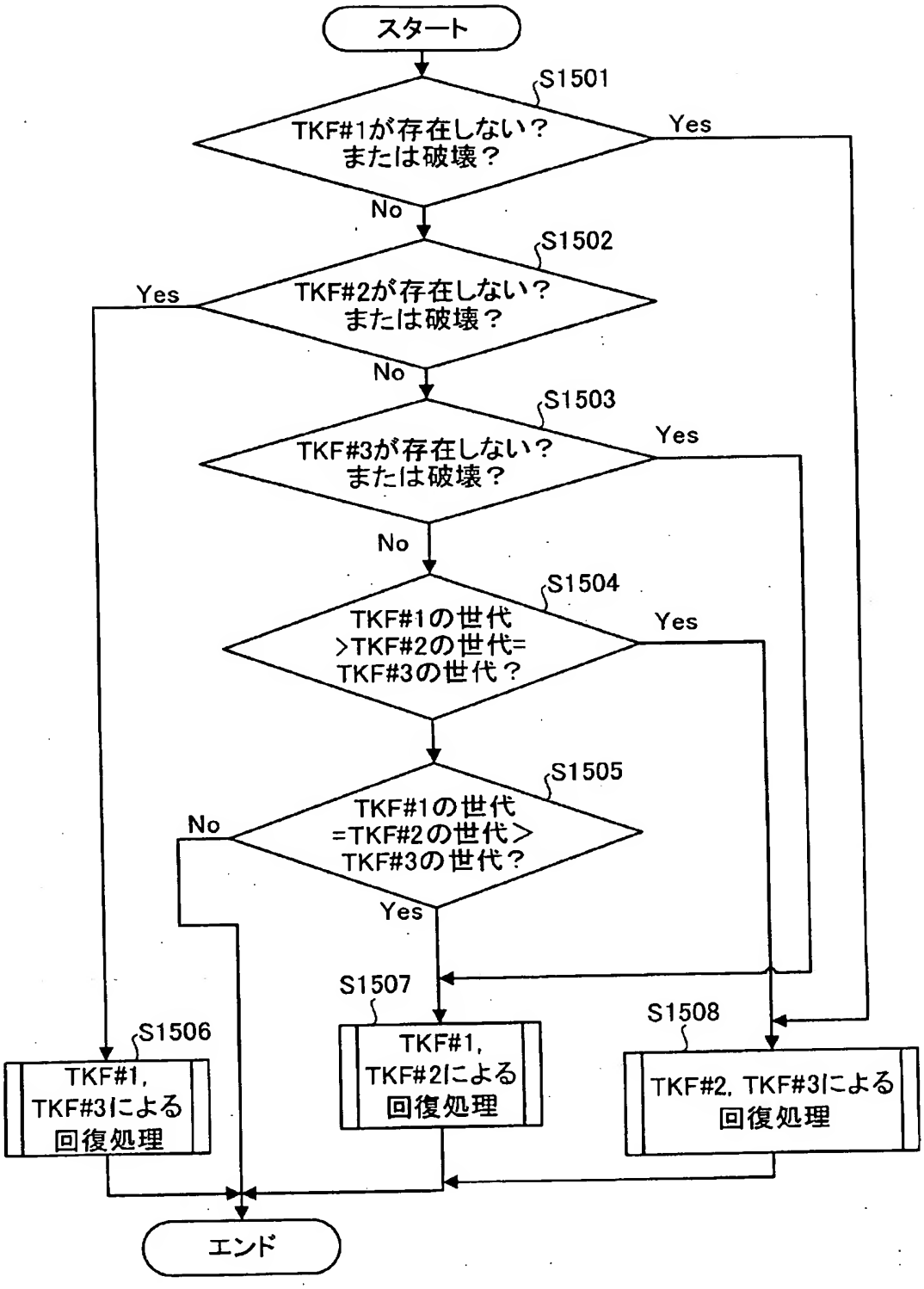
【図１３】


スタート
TKF1，TKF2を乱数生成
S1301
世代を乱数生成
S1302
ドライブ部から乱数1(BN1)を取得
S1303
BN1とTKFN2からTKFの全タイトルキーを暗号化して
暗号化タイトルキー(ETK1)を生成
S1304
BN1とTKFN1と世代とETK1からTKF#1を生成
S1305
BN1とTKF#1を記録媒体に書き込み
S1306
ドライブ部から乱数2(BN2)を取得
S1307
BN2とTKFN1からTKFの全タイトルキーを暗号化
暗号化タイトルキー(ETK2)を生成
S1308
BN2とTKFN2と世代とETKF2からTKF#2を生成
S1309
BN2とTKF#2を記録媒体に書き込み
S1310
ドライブ部から乱数3(BN3)を取得
S1311
BN3と世代とTKFN1とTKFN2からTKF#3を生成
S1312
BN3とTKF#3を記録媒体に書き込み
S1313
エンド

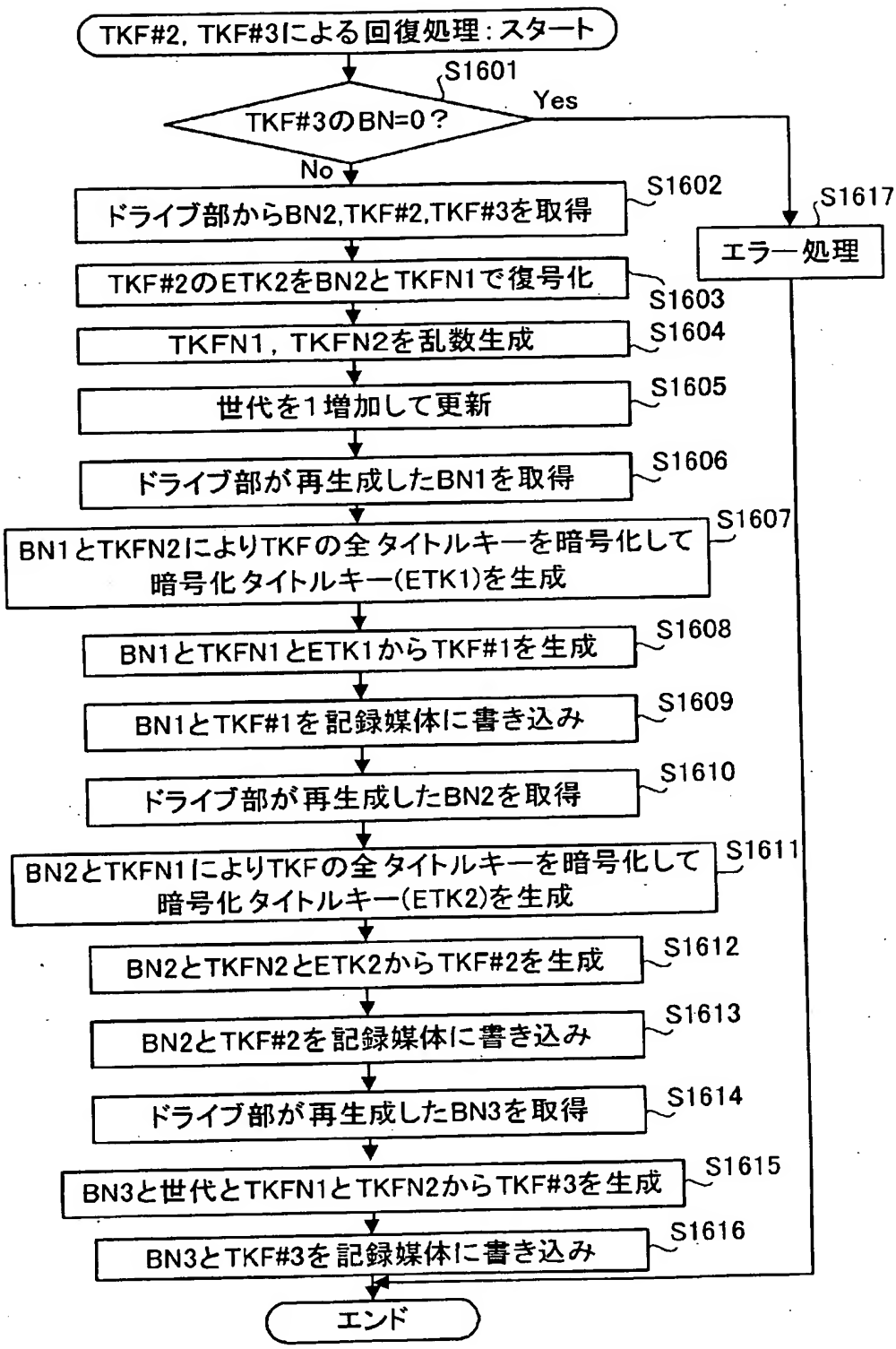
【図１４】


スタート
BN1をドライブ部から取得
S1401
TKF#1のETK1をBN1とTKFN2で復号化
S1402
TKFN1,TKFN2を乱数生成
S1403
世代を1増加して更新
S1404
ドライブ部が再生成したBN1を取得
S1405
BN1とTKFN2によりTKFの全タイトルキーを暗号化して
暗号化タイトルキー(ETK1)を生成
S1406
BN1と世代とTKFN1とETK1からTKF#1を生成
S1407
BN1とTKF#1を記録媒体に書き込み
S1408
ドライブ部が再生成したBN2を取得
S1409
BN2とTKFN1によりTKFの全タイトルキーを暗号化して
暗号化タイトルキー(ETK2)を生成
S1410
BN2とTKFN2と世代とETK2からTKF#2を生成
S1411
BN2とTKF#2を記録媒体に書き込み
S1412
ドライブ部が再生成したBN3を取得
S1413
BN3と世代とTKFN1とTKFN2からTKF#3を生成
S1414
BN3とTKF#3を記録媒体に書き込み
S1415
エンド

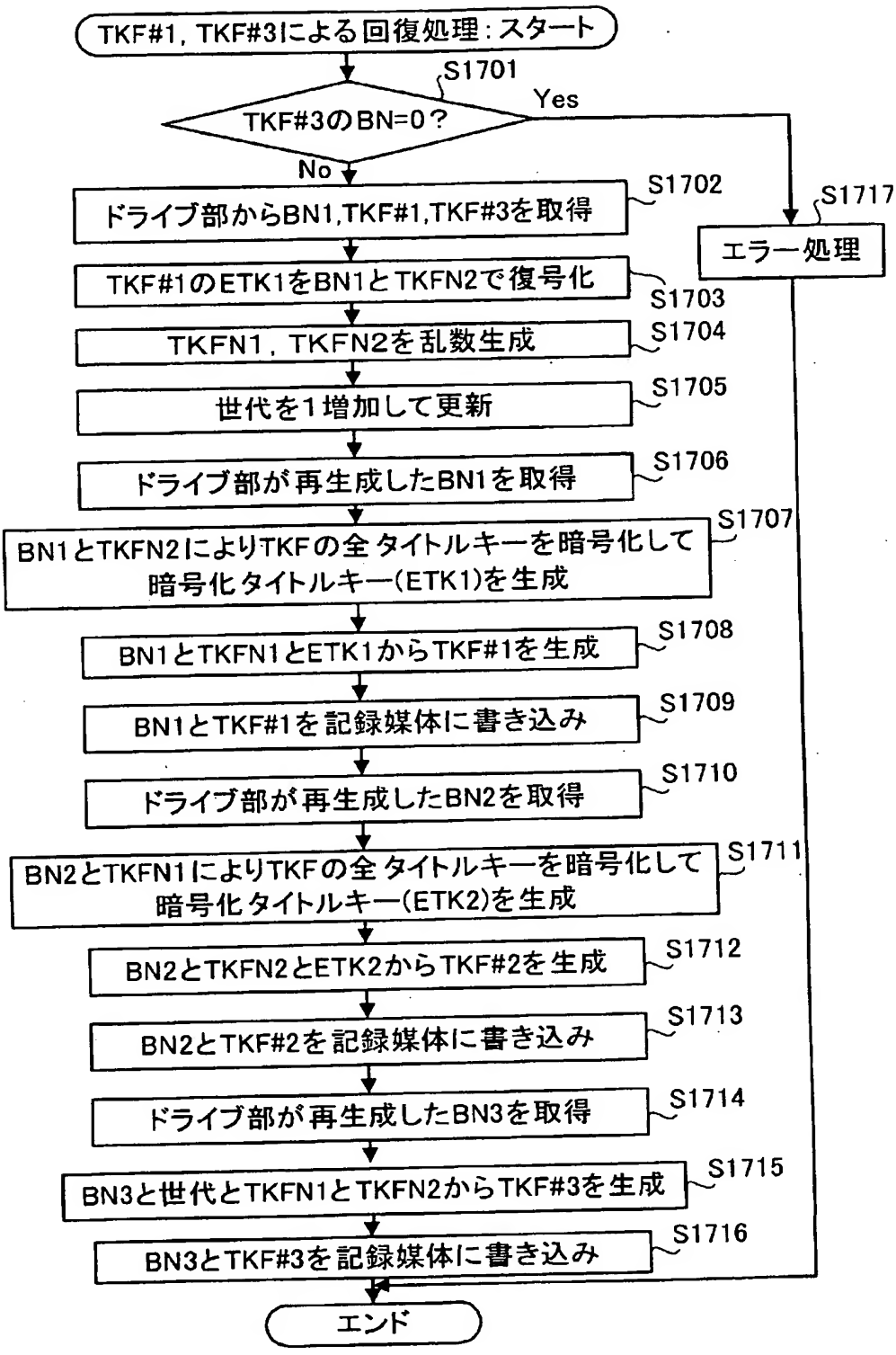
【図１５】


スタート
S1501
TKF#1が存在しない？
または破壊？
Yes
No
S1502
TKF#2が存在しない？
または破壊？
Yes
No
S1503
TKF#3が存在しない？
または破壊？
Yes
No
S1504
TKF#1の世代
>TKF#2の世代=
TKF#3の世代？
Yes
S1505
TKF#1の世代
=TKF#2の世代>
TKF#3の世代？
No
Yes
S1506
TKF#1,
TKF#3による
回復処理
S1507
TKF#1,
TKF#2による
回復処理
S1508
TKF#2, TKF#3による
回復処理
エンド

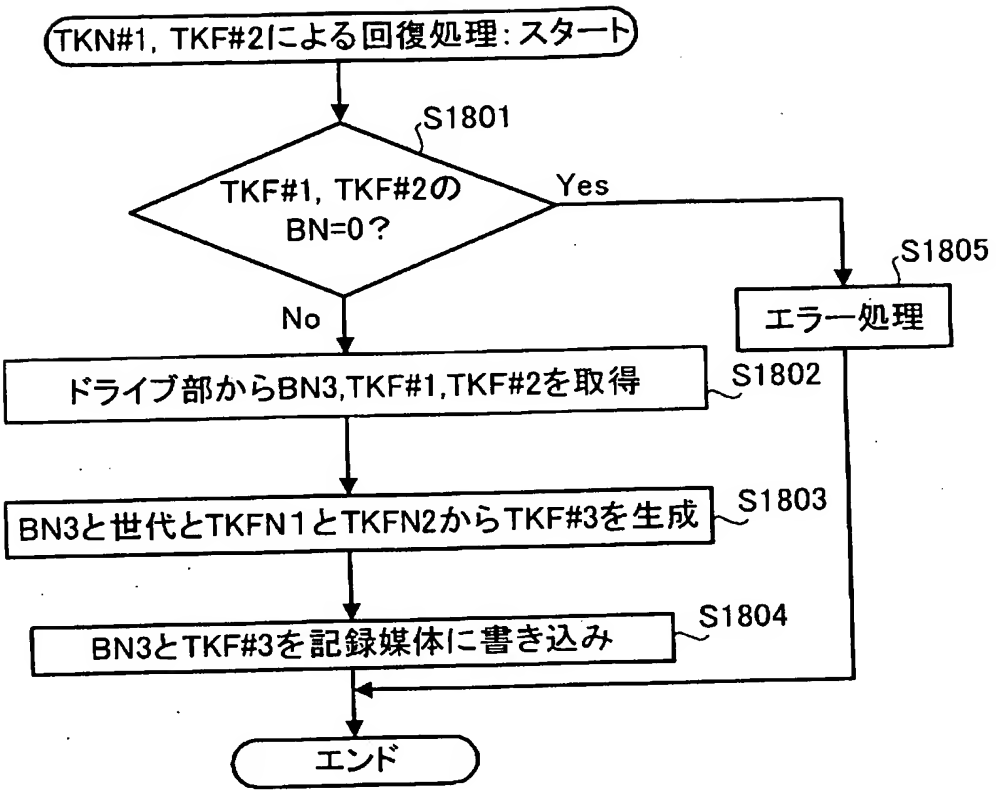
【図１６】


TKF#2, TKF#3による回復処理：スタート
S1601
TKF#3のBN=0？
Yes
No
S1602
ドライブ部からBN2,TKF#2,TKF#3を取得
S1617
エラー処理
TKF#2のETK2をBN2とTKFN1で復号化
S1603
TKFN1，TKFN2を乱数生成
S1604
世代を1増加して更新
S1605
ドライブ部が再生成したBN1を取得
S1606
BN1とTKFN2によりTKFの全タイトルキーを暗号化して暗号化タイトルキー(ETK1)を生成
S1607
BN1とTKFN1とETK1からTKF#1を生成
S1608
BN1とTKF#1を記録媒体に書き込み
S1609
ドライブ部が再生成したBN2を取得
S1610
BN2とTKFN1によりTKFの全タイトルキーを暗号化して暗号化タイトルキー(ETK2)を生成
S1611
BN2とTKFN2とETK2からTKF#2を生成
S1612
BN2とTKF#2を記録媒体に書き込み
S1613
ドライブ部が再生成したBN3を取得
S1614
BN3と世代とTKFN1とTKFN2からTKF#3を生成
S1615
BN3とTKF#3を記録媒体に書き込み
S1616
エンド

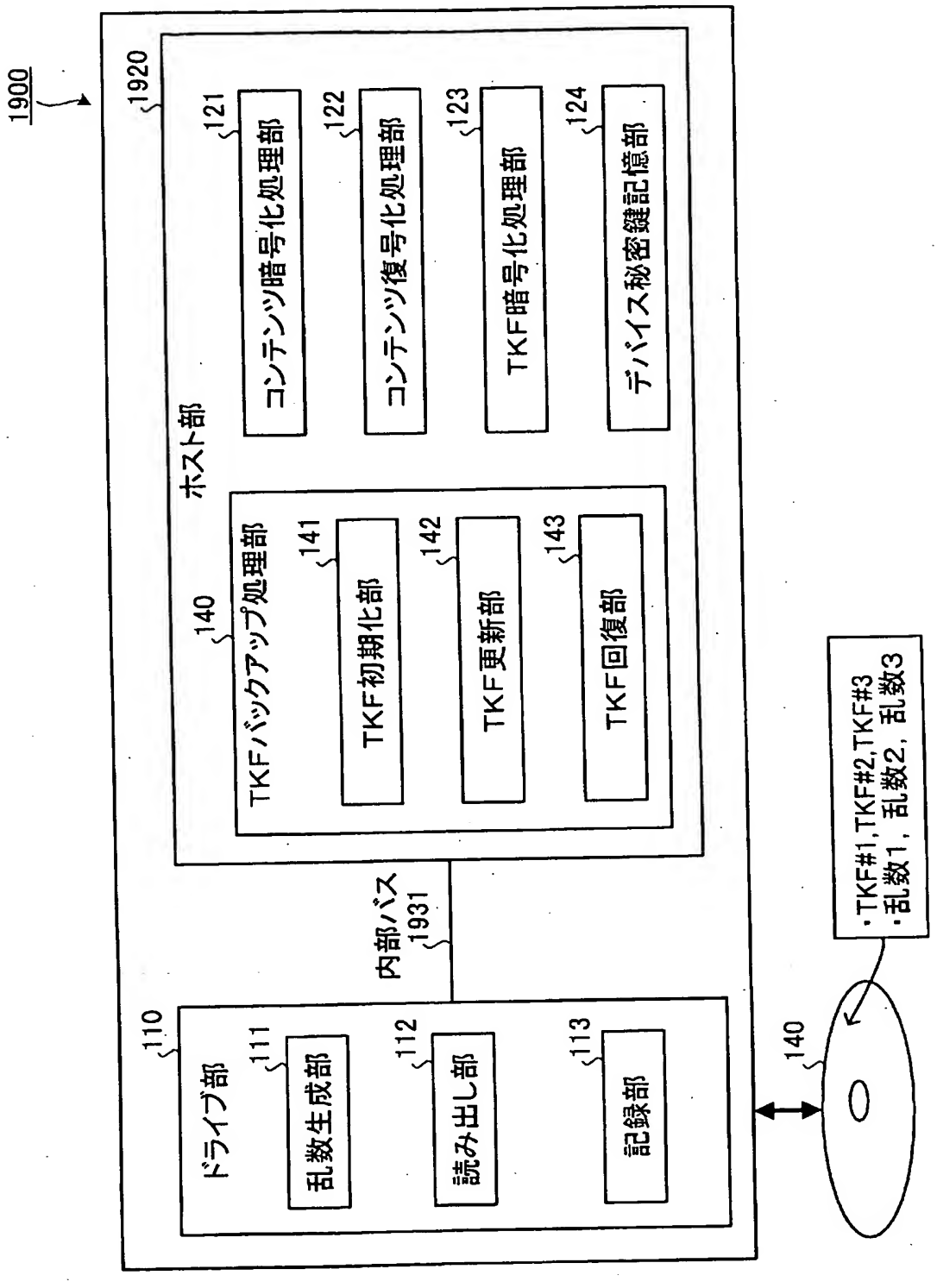
【図１７】


TKF#1, TKF#3による回復処理：スタート
S1701
TKF#3のBN=0？
Yes
No
S1717
エラー処理
S1702
ドライブ部からBN1,TKF#1,TKF#3を取得
S1703
TKF#1のETK1をBN1とTKFN2で復号化
S1704
TKFN1，TKFN2を乱数生成
S1705
世代を１増加して更新
S1706
ドライブ部が再生成したBN1を取得
S1707
BN1とTKFN2によりTKFの全タイトルキーを暗号化して
暗号化タイトルキー(ETK1)を生成
S1708
BN1とTKFN1とETK1からTKF#1を生成
S1709
BN1とTKF#1を記録媒体に書き込み
S1710
ドライブ部が再生成したBN2を取得
S1711
BN2とTKFN1によりTKFの全タイトルキーを暗号化して
暗号化タイトルキー(ETK2)を生成
S1712
BN2とTKFN2とETK2からTKF#2を生成
S1713
BN2とTKF#2を記録媒体に書き込み
S1714
ドライブ部が再生成したBN3を取得
S1715
BN3と世代とTKFN1とTKFN2からTKF#3を生成
S1716
BN3とTKF#3を記録媒体に書き込み
エンド

【図１８】


TKN#1, TKF#2による回復処理：スタート
S1801
TKF#1, TKF#2の
BN=0？
Yes
No
S1805
エラー処理
ドライブ部からBN3,TKF#1,TKF#2を取得
S1802
BN3と世代とTKFN1とTKFN2からTKF#3を生成
S1803
BN3とTKF#3を記録媒体に書き込み
S1804
エンド

【図１９】


1900
1920
ホスト部
121
コンテンツ暗号化処理部
122
コンテンツ復号化処理部
123
TKF暗号化処理部
124
デバイス秘密鍵記憶部
140
TKFバックアップ処理部
141
TKF初期化部
142
TKF更新部
143
TKF回復部
内部バス
1931
110
ドライブ部
111
乱数生成部
112
読み出し部
113
記録部
140
・TKF#1,TKF#2,TKF#3
・乱数1，乱数2，乱数3

【書類名】要約書
【要約】
【課題】タイトルキーファイルの復元を確実に行い、第三者によるコンテンツの不正な復元を防止すること。
【解決手段】複数のタイトルコンテンツを暗号化するタイトルキーが登録されたタイトルキーファイルと、タイトルキーによって暗号化されたタイトルコンテンツとが記録された記録媒体の記録・再生を行うコンテンツ記録再生装置であって、タイトルキーファイルを生成して記録媒体に記録するＴＫＦ初期化部１４１と、複数のタイトルキーファイルのそれぞれに対応した第１の乱数を生成する乱数生成部１１１と、複数のタイトルキーファイルをＤＶＤメディア１４０に記録する記録部１１３とを備え、ＴＫＦ初期化部１４１は、タイトルキーファイルのそれぞれを、第１の乱数と関連づけられた他のタイトルキーファイルに登録された第２の乱数とによってタイトルキーを暗号化した暗号化タイトルキーと第１の乱数と第２の乱数とを登録する。
【選択図】　図１

出願人履歴

０００００３０７８
20010702
住所変更
５９９１３７０１３

東京都港区芝浦一丁目１番１号
株式会社東芝
３０１０６３４９６
20031101
住所変更
５０３３６２８９８

東京都港区芝浦一丁目１番１号
東芝ソリューション株式会社